UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA
ESCUELA DE ELECTRÓNICA Y TELECOMUNICACIONES

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP

Tesis previa a la obtención del Título de Ingeniero en Electrónica y Telecomunicaciones

AUTORES:

Clavijo Zhindón Christian Andrés

Montenegro Salinas Cristian Fernando

Muñoz Palomeque Marco Oswaldo

DIRECTOR:

Ing. Lizandro Damián Solano Quinde, PhD

CUENCA-ECUADOR
2014

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

RESUMEN

Este proyecto presenta el diseño e implementación de un sistema de seguridad residencial a nivel prototipo, que permite el monitoreo del estado de los sensores, video vigilancia, almacenamiento y control de eventos, a través de la red de ETAPA EP.

En el sistema se implementó de manera íntegra la aplicación de la Central de Alarma y el panel de usuario, así como las aplicaciones de software para los diferentes tipos de usuarios que utilizan el sistema. El sistema permite notificar al usuario en caso que se genere algún evento. Además, los clientes pueden tener acceso visual a las cámaras instaladas y gestión de los sensores instalados en su hogar tanto de manera remota como local. El prototipo se diseñó para funcionar a través de internet, sin embargo, como implementación futura se debe disponer de un canal dedicado en la red de ETAPA EP para que no interfiera con los otros servicios contratados por el cliente e incrementar la seguridad.

Palabras Claves:

Seguridad, Video Vigilancia, Alarma, Monitoreo, Remoto, ETAPA EP, Internet.

ABSTRACT

This project is intended to design and implement a prototype home security system, which allows local and remote alarm monitoring, events storage and handling, and video surveillance through the ETAPA EP network.

All the hardware in the central alarm and user's interface was entirely implemented in the system. There were also specific web application interfaces developed for all the different users that take part in the system. The client is notified if an alarm is generated due to the system having databases which record the current sensors' state and a communication protocol set between the central alarm and the server side through the network. As a future implementation, it is necessary to have an independent channel in the ETAPA EP network to communicate, in order to not interfere with other contracted services. Clients will be able to control the system remotely (Internet) or locally and they can have visual access to their cameras installed at home.

Key Words:

Security, Video Monitoring, Alarm, Monitoring, Remotely, ETAPA EP, Internet.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

ÍNDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

Yo, Christian Andrés Clavijo Zhindon, autor de la tesis "IMPLEMENTACIÓN Y DESARROLLO DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Ingeniero en Electrónica y Telecomunicaciones. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 10 de Noviembre de 2014

Christian Andrés Clavijo Zhindon
C.I: 0302089164

Yo, Cristian Fernando Montenegro Salinas, autor de la tesis "IMPLEMENTACIÓN Y DESARROLLO DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Ingeniero en Electrónica y Telecomunicaciones. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 10 de Noviembre de 2014

Cristian Fernando Montenegro Salinas
C.I: 1400661573

Yo, Marco Oswaldo Muñoz Palomeque, autor de la tesis "IMPLEMENTACIÓN Y DESARROLLO DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Ingeniero en Electrónica y Telecomunicaciones. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 10 de Noviembre de 2014

Marco Oswaldo Muñoz Palomeque

C.I: 0104141791

Yo, Cristian Andrés Clavijo Zhindon, autor de la tesis ""IMPLEMENTACIÓN Y DESARROLLO DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP",", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 10 de Noviembre de 2014

Christian Andrés Clavijo Zhindon
C.I: 0302089164

Yo, Montenegro Salinas Cristian Fernando, autor de la tesis "DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 10 de Noviembre de 2014

Cristian Fernando Montenegro Salinas

C.I: 1400661573

Yo, Marco Oswaldo Muñoz Palomeque, autor de la tesis ""IMPLEMENTACIÓN Y DESARROLLO DE UN SISTEMA PROTOTIPO DE SEGURIDAD RESIDENCIAL A TRAVÉS DE LAS REDES DE ETAPA EP",", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 10 de Noviembre de 2014

Marco Oswaldo Muñoz Palomeque

C.I: 0104141791

Agradecimiento

A la Universidad de Cuenca, porque en sus aulas, recibimos el conocimiento intelectual y humano de cada uno de los docentes de la Escuela de Electrónica y Telecomunicaciones.

Agradecemos a todas las personas que de una u otra forma estuvieron con nosotros, porque cada una aportó de cierta manera para la realización de ésta tesis; y es por ello que a todos y a cada uno de ustedes les dedicamos todo el esfuerzo, sacrificio y tiempo entregado en el desarrollo de esta tesis.

Especial agradecimiento a nuestro Director de Tesis el PhD. Lizandro Solano Quinde por su apoyo, consejos y amistad.

Los Autores

DEDICATORIA

Esta tesis la dedico a Dios quién ha sabido guiarme siempre por el buen camino.

A mis padres por su apoyo, consejos, comprensión en los momentos difíciles, y por brindarme los recursos necesarios para poder realizar mis estudios. Ellos me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia y el coraje para conseguir mis objetivos.

A mis hermanas por estar siempre presentes, acompañándome para poderme realizar profesionalmente.

A los profesores que con sus consejos supieron darme la fuerza para seguir adelante y no caer ante los problemas que se presentaban, enseñándome a enfrentar las adversidades sin perder nunca la dignidad ni decaer en el intento.

Christian

DEDICATORIA

A Dios, por siempre estar ahí cuando lo necesitaba y ser la fuerza para seguir día a día.

A mis padres por el esfuerzo y apoyo realizado durante mis años de estudio.

A mis hermanos por su apoyo incondicional.

A mis amigos y compañeros de tesis (Christian y Cristian) por el esfuerzo realizado durante el desarrollo de esta tesis.

Marco

DEDICATORIA

Esta tesis la dedico a Dios quién ha sido la guía y el camino para ser un hombre de bien.

A mi hija que es la luz que ilumino mi vida desde el momento que nació y a quien le dedico mi vida entera.

A mi esposa por ser mi compañera y apoyo en la travesía de la vida y que me permitieron enfrentar las dificultades que se presentar sin decaer en ningún momento.

A mis padres y hermana por su comprensión y apoyo todo el tiempo, brindándome los recursos necesarios para culminar mis estudios.

Fernando

CAPÍTULO 1

INTRODUCCIÓN

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 1 INTRODUCCION

1.1 Introducción

Para el desarrollo del prototipo se plantea un esquema con tres etapas, como se muestra en la Figura 1-1:

Figura 1-1: Etapas de desarrollo del prototipo

La etapa “Aplicación cliente” hace referencia a los dispositivos electrónicos instalados en el domicilio del cliente, los mismos que son los encargados de monitorear los eventos generados en el domicilio, como por ejemplo la presencia de una persona.

En la etapa “Aplicación servidor” se instalaran los servidores necesarios según los requerimientos del prototipo y se desarrollará la aplicación web encargada de gestionar el sistema de seguridad instalado en el domicilio del cliente.

Finalmente, debido a que los dispositivos electrónicos y las aplicaciones ejecutándose en el servidor tienen que intercambiar información, en la etapa “Medio de Comunicación” se analiza la red de ETAPA EP y la seguridad de la misma.

El presente documento incluye un capítulo para cada etapa antes descrita, donde se detalla los requerimientos del sistema, el planteamiento de la solución, y los esquemas y diseños necesarios. Además, se cuenta con un capítulo dedicado a la implementación de la aplicación total. A continuación se describe cada uno de los ellos.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Capítulo 3

En este punto se detalla la estructurada la red de transmisión de ETAPA EP, los requerimientos de red en cada nivel del desarrollo del proyecto, además, se realiza un análisis de las vulnerabilidades de la red y las soluciones para mitigarlos.

Capítulo 4

En la etapa “Aplicación cliente” se realiza un análisis de la situación actual para determinar una aplicación tentativa definida de manera general. Se determinan los protocolos y medios de transmisión a utilizar y finalmente se describe la aplicación de una manera más específica.

Capítulo 5

En este capítulo se analiza los requerimientos necesarios en la parte de software a fin de determinar el sistema operativo, lenguajes de programación, APIs y servidores de manera que brinden un soporte eficiente a las aplicaciones a ser desarrolladas. Será necesario el desarrollo de una aplicación que se encargue de la gestión del sistema de seguridad, manejo e interpretación de los datos generados por los dispositivos electrónicos, y el almacenamiento de video e información de los usuarios del sistema en los servidores respectivos. Además, es necesario el desarrollo de una aplicación que se encargue de la comunicación con la central de alarmas instalada en el domicilio del cliente.

Capítulo 6

Se describe la implementación del prototipo, desde la instalación de servidores, sistema operativo, aplicaciones, hasta la configuración y pruebas de funcionamiento.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Capítulo 7

Se detallan los costos de recursos utilizados durante el desarrollo del prototipo, determinando el precio final y una comparación general de costos del prototipo con otros sistemas de seguridad en el mercado.

Capítulo 8

En este último capítulo se desarrollan las conclusiones y recomendaciones basadas en la realización del proyecto de tesis.

1.2 Justificación de la Investigación

En la actualidad, las empresas de seguridad domiciliarias brindan servicios de alarma y video vigilancia. La primera utilizando la red PSTN y GSM, y la segunda a través de Internet, trabajando cada una por separado, lo que limita la capacidad del servicio y la interacción e interface presentada a los usuarios. Las redes TCP/IP brindan un alto grado de interacción extremo a extremo, siendo apropiadas para unir estos dos servicios.

ETAPA EP a futuro desplegará su red de fibra óptica donde, se estima que; en promedio tendrá velocidades de 19 Mbps y 38 Mbps para carga y descarga, respectivamente. Por otro lado aproximadamente un 96% de clientes de Internet tienen contratado planes menores a 10 Mbps, teniendo en promedio 9 Mbps de capacidad en la red para brindar otros tipos de servicios, como por ejemplo el servicio de seguridad domiciliaria.

De esta forma, las redes de fibra óptica serán aprovechadas para consolidar los servicios de alarma y video vigilancia beneficiándose de las capacidades y velocidades que brindan estas redes.

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Diseñar e Implementar un Sistema de Seguridad residencial a nivel de prototipo, que permita el monitoreo y control de sensores, video vigilancia, almacenamiento de eventos, a través de la red de ETAPA EP.

1.3.2 Objetivos específicos

- Analizar la red de ETAPA EP para establecer los requerimientos para la comunicación entre la red de acceso de los clientes y los servidores del sistema de seguridad.
- Analizar la seguridad del sistema y plantear soluciones a los posibles riesgos.
- Diseñar e Implementar la aplicación prototipo de cliente, lo cual incluye: conectividad del sistema de alarmas, monitoreo y video vigilancia.
- Diseñar e implementar la aplicación prototipo de servidor que permita gestionar el sistema de manera local o remota, almacenamiento de información, gestión de clientes y monitoreo general.
- Analizar los costos requeridos para la implementación del sistema.

1.4 Alcances

En el presente proyecto de tesis se diseñará e implementará un sistema de seguridad residencial a nivel de prototipo, que permita el monitoreo de sensores, video vigilancia, almacenamiento de eventos y control, a través de la red de ETAPA EP.

La funcionalidad del sistema incluye:

- Monitoreo del estado de los sensores mediante interfaces, las cuales están desarrolladas para los diferentes tipos de

usuarios que conforman el sistema, tales como: cliente, administrador y la central de monitoreo.

- Notificación al usuario en caso de que alguna alarma se genere, mediante el método elegido para éste propósito, tales como: llamada telefónica, correo electrónico, etc.
- Implementación de bases de datos, en las cuales se almacenan los registros y estados actuales de los sensores.
- Acceso visual a las cámaras instaladas en su domicilio, donde en el caso de que se produzca algún evento, el video capturado será almacenado.
- Conexión remota (a través de internet) o local (a través de la central de alarma) al sistema para monitorear el estado actual de los sensores.

Las pruebas del sistema se realizarán a nivel de laboratorio, a fin de verificar la funcionalidad del sistema. Las pruebas finales serán realizadas con la infraestructura de ETAPA EP con el fin de obtener resultados reales.

CAPÍTULO 2

BASES TEÓRICAS

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 2 BASES TEORICAS

2.1 Conceptos de seguridad electrónica y domiciliaria

2.1.1 Seguridad Domiciliaria

Conjunto estratégico de recursos humanos y tecnológicos que brindan tranquilidad a los usuarios de situaciones que representan un peligro o malestar para los mismos. [1]

2.1.2 Seguridad Electrónica

Es la parte tecnológica que se encarga de monitorear el domicilio de manera permanente y alertar al usuario de la ocurrencia de un evento. Los sistemas electrónicos de seguridad son pasivos, lo que significa que no son capaces de evitar eventos, solo los detecta y reporta. [1]

2.2 Sistema de Alarma

2.2.1 Funcionamiento del Sistema de Alarma

El sistema de alarma consiste en un equipo central que gestiona los sensores conectados a él, y a través de un sistema de comunicaciones como telefonía fija, telefonía móvil o internet alerta al usuario de eventos ocurridos. [1]

Las funciones del sistema de alarma son:

- Monitoreo de los sensores.
- Gestión de la energía del sistema.
- Comunicación con el usuario.
- Comunicación con entidades de monitoreo.
- Generación de señales de auxilio.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

2.2.2 Partes de un sistema de alarma

Central de Alarma: Es el equipo central del sistema, lleva incorporado un procesador que gestiona el funcionamiento general del sistema. Conformado por los siguientes elementos:

- **Sensores**: Su función es detectar la presencia de intrusos o eventos en el domicilio. Existe una amplia gama de sensores sin embargo los más utilizados son los de detección On-Off.

- **Interface–Usuario:** Dispositivos que permiten la interacción del usuario con el sistema, existen diversos dispositivos electrónicos y varían según los servicios prestados y la facilidad de uso. Por ejemplo Teclado LCD icono, Teclado 555 LED, etc.

- **Sistema de Gestión de Batería:** Gestiona la energía de la red eléctrica y de la batería en caso de corte de energía, con el fin de preservar el tiempo de vida de la batería y brindar servicio ininterrumpido.

- **Sirena:** Existen varias formas de alertar la presencia de intrusos, una de estas utilizada ampliamente es la sirena. Su función es alertar mediante ondas sonoras de alta potencia la ocurrencia de un evento en el lugar monitoreado.

En la Figura 2-1 se muestran varios componentes de un kit de alarma básico, donde el Panel de Alarma corresponde a la Central de Alarma, el sistema de gestión de batería comprende parte de la central de alarma, la batería y el transformador. El suiche liviano y el detector de movimiento son los sensores y el teclado LED es parte de la interface de usuario, y por último la sirena o llamada también parlante. [1]

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Figura 2-1: Componentes de un sistema de alarma. (Tomado de [1])

2.3 Redes TCP-IP

2.3.1 Transmisión de datos en Internet

Internet es una herramienta que facilita la comunicación, y está formada por varias redes LAN y WAN, donde se utilizan varios protocolos de comunicación resaltando entre ellos TCP/IP. [2]

2.3.2 Modelo de Referencia OSI

"Modelo de Referencia OSI, desarrollado por la ISO (International Standard Organisation), como una guía para definir un conjunto de protocolos abiertos. Su finalidad es proporcionar una base común para la coordinación en el desarrollo de normas destinadas a la interconexión de sistemas, permitiendo a la vez situar las normas existentes en la perspectiva del modelo de referencia global." [3]

El modelo de referencia OSI propone 7 capas donde se determinan sus funcionalidades y que se describen a continuación:

- **Capa Física:** Se encarga de gestionar el hardware y las señales físicas de comunicación sean éstas eléctricas o electromagnéticas, etc.

- **Capa de Enlace:** Controla el enlace de datos, a través de técnicas como sincronización y control de errores.
- **Capa de Red:** Provee mecanismos para identificar a los dispositivos en la red y determinar los caminos para el envío de paquetes (enrutamiento).
- **Capa de Transporte:** Gestiona el control de flujo de la información de extremo a extremo y ofrece comunicaciones seguras y rápidas.
- **Capa Sesión:** Brinda servicios a la capa de presentación para establecer sesiones en la comunicación.
- **Capa de Presentación**: Provee servicios a la capa de aplicación para interpretar los datos de la manera correcta.
- **Capa de Aplicación:** Se encarga de interactuar con el usuario y ofrecer servicios al destino final.

2.3.3 Pila de protocolos TCP/IP

Es un conjunto de protocolos que trabajan en redes de comunicación, siendo los más utilizados TPC e IP.

TCP (Protocolo de Control de Transmisiones): Corresponde a la capa de transporte del modelo de referencia OSI. Una de sus funciones principales es controlar el flujo de la información. Existen varios parámetros para definir el paquete de este protocolo: puerto origen, puerto destino, número de secuencia, señales de confirmación, tamaño, bits de control, windows, check zoom, punteros, etc.

IP (Protocolo de Internet): Corresponde a la capa de red del modelo de referencia OSI. Una de sus funciones principales es la identificar el host de origen y destino en la comunicación y asegurar el correcto enrutamiento de los paquetes. Los parámetros son la dirección IP local, la dirección IP remota, el gateway y la red. [2]

2.4 Arquitectura Cliente Servidor

Esta arquitectura está formada por un equipo servidor quien está a la espera de peticiones y uno o varios equipos cliente que se comunican con el servidor para solicitar servicios. [4]

2.5 Software para desarrollo de aplicaciones en dispositivos electrónicos

Para el desarrollo de aplicaciones electrónicas se utiliza diferente tipos de software, cada uno de ellos con diferentes funcionalidades según la etapa de desarrollo en la que se encuentre.

Para la etapa de programación se utiliza MikroC PRO for PIC, el mismo que genera un archivo *.hex*. En la etapa de implementación se necesita realizar la escritura del programa en el microcontrolador, siendo Pickit 2 el software encargado de traducir código hexadecimal a código máquina. [5]

MikroC PRO for PIC: Es un IDE utilizado para la programación de microcontroladores, la programación se realiza en lenguaje C, el cual ofrece una gran variedad de librerías que agilitan la programación. Soporta una gran variedad de microcontroladores entre ellos PIC de microchip. [6]

Pickit 2: Es un software utilizado para descargar programas en microcontroladores. Dispone de un equipo de hardware para realizar la escritura del programa en el microcontrolador.

2.6 Software Comercial

El software comercial es aquel software, libre o no, que es comercializado, es decir, que existen sectores de la economía que lo sostiene a través de su producción, su distribución o soporte. [7]

Este software implica una transacción monetaria desde el usuario final a la firma desarrolladora. La mayoría del software comercial es propietario, donde el usuario final adquiere junto con el software, una

licencia de uso para un solo ordenador o licencia múltiple para varios ordenadores. La distribución no autorizada está penalizada por la ley.

Ventajas

- El software comercial cuenta con más opciones desarrolladas y soporte general de la industria.
- El software comercial ofrece beneficios en construcción de aplicaciones a medida que la complejidad aumenta.

Desventajas

- Es ilegal extender una pieza de software comercial para adaptarla a las necesidades particulares de un problema específico.
- La innovación es derecho exclusivo de la compañía fabricante. Es ilegal hacer copias del software propietario sin antes haber contratado las licencias necesarias.

2.7 Software Libre

También llamado *free software*, denominación que se le da al software que respeta la libertad de los usuarios, individual o colectivamente, para hacer lo que quieran con él. Esto incluye la libertad para redistribuir el software de manera gratuita o pagada. [8]

Ventajas

- Brinda libertad a sus usuarios.
- Puede ser usado, copiado, modificado y redistribuido.
- Ahorro considerable en la adquisición de licencias.
- Tiende a ser eficiente.
- Disminuye el índice de software pirata.

Desventajas

- El software libre tiende a ser incompatible con el software comercial.
- El software libre crea riesgos legales.
- El software libre no tiene garantía proveniente del autor

2.8 HTTP.

Es un protocolo de red para publicar páginas web, generalmente implementado sobre TCP/IP. HTTP es la base sobre la cual está fundamentado Internet. El protocolo HTTP es un protocolo que funciona a través de solicitudes (request) y respuestas (response) entre un cliente y un servidor. A una secuencia de estas solicitudes se le conoce como sesión HTTP. A menudo las peticiones tienen que ver con archivos, ejecución de un programa, consulta a una base de datos, traducción y otras funcionalidades. [9]

2.9 Sockets

Un socket se define como el punto final en una conexión. Los sockets se crean y se utilizan con un sistema de peticiones y una interface de programación de aplicación de sockets (API). Los sockets constituyen una interface de programación de aplicaciones. Permiten la comunicación entre programas a través de una red TCP/IP. [10]

Toda conexión de red que entra y sale de un computador queda identificada de forma única por la combinación de dos números: la dirección IP del computador y el número de puerto utilizado, que unidos componen lo que se conoce como socket.

2.10 Lenguaje de Programación Java

Java es un lenguaje de programación orientado a objetos desarrollado por Sun Microsystems. El lenguaje toma mucha de su sintaxis de C y C++, pero posee un modelo de objetos más simple, además, elimina herramientas de bajo nivel, que suelen conducir a errores, como la

manipulación directa de punteros o memoria. Con respecto a la memoria, su gestión no es un problema ya que ésta es gestionada por el propio lenguaje y no por el programador. [11]

Una de las principales características para la popularidad de Java es el hecho de ser un lenguaje independiente de la plataforma. La característica multiplataforma se consigue debido a que se ha creado una Máquina de Java para cada sistema, que se encarga de realizar un puente entre el sistema operativo y el programa Java, haciendo que estos se entiendan correctamente.

2.11 Servidor de Aplicaciones

Un servidor de aplicaciones opera la mayoría de las transacciones relacionadas con la lógica y el acceso de datos de la aplicación. La ventaja principal de un servidor de aplicaciones es la facilidad para el desarrollo de aplicaciones.

Proporciona servicios que soportan la ejecución y disponibilidad de las aplicaciones. Provee servicios de “middleware”, es decir, trabaja como un intermediario para la seguridad, mantenimiento, intercomunicación con variados servicios, para efectos de confiabilidad, etc., además de proveer el acceso a datos.

Como consecuencia del éxito del lenguaje de programación Java el término servidor de aplicaciones se ha convertido en sinónimo de la plataforma Java EE (J2EE) de Sun Microsystems.

Java EE proporciona estándares que permiten a un servidor de aplicaciones servir como “contenedor” de los componentes que conforman las aplicaciones. Estos componentes, escritos en lenguaje Java, usualmente se conocen como Servlets, Java Server Pages (JSPs) y Enterprise JavaBeans (EJBs) y permiten implementar diferentes capas de aplicación, como la interface de usuario, la lógica de negocio, la gestión de sesiones de usuario o el acceso a bases de datos remotas. [12]

El estándar Java EE permite el desarrollo de aplicaciones de empresa de una manera sencilla y eficiente. Una aplicación desarrollada con las tecnologías Java EE permite ser desplegada en cualquier servidor de aplicaciones o servidor web que cumpla con el estándar. Un servidor de aplicaciones es una implementación de la especificación Java EE.

La arquitectura Java EE es la que se observa en la Figura 2-2:

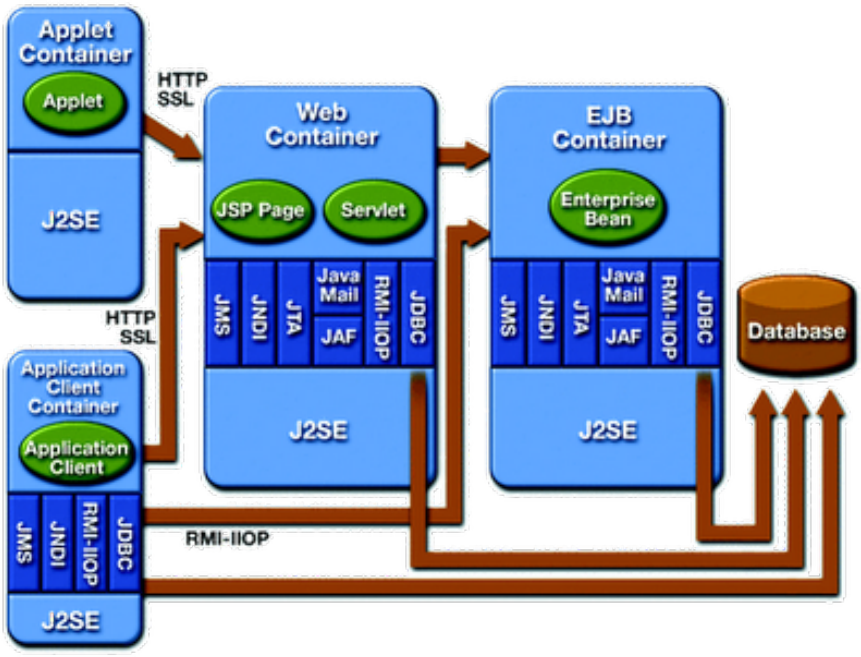


Figura 2-2: Arquitectura Java EE. (Tomado de [12])

A continuación se definen algunos de los conceptos que aparecen en la Figura 2-2:

- ***Cliente Web (****Applet Container****):*** Es usualmente un navegador o interactúa con el contenedor web haciendo uso de HTTP. Recibe páginas HTML o XML y puede ejecutar applets y código javascript.
- ***Aplicación cliente web:*** Son clientes que no se ejecutan dentro de un navegador y pueden utilizar cualquier tecnología para comunicarse con el contenedor web o directamente con la base de datos.

- **Contenedor web (Web Container):** Comúnmente denominado servidor web, es la parte visible del servidor de aplicaciones. Utiliza los protocolos HTTP y SSL (seguro) para comunicarse.
- **Servidor de aplicaciones:** Proporciona servicios que soportan la ejecución y disponibilidad de las aplicaciones desplegadas. Es el corazón de un gran sistema distribuido.

Existe una variedad de implementaciones de Java EE, cada una con sus propias características que la puedan hacer más atractiva en el desarrollo de un determinado sistema. Algunas de las implementaciones más utilizadas son las siguientes:

- GlassFish
- BEA WebLogic
- JBoss
- IBM WebSphere
- Sun Netscape IPlanet
- Sun One
- Oracle IAS
- Borland AppServer.

2.12 Página Web

Se considera una página web, conocida también como página de internet, a un documento que se encuentra disponible en Internet, codificado según sus estándares y con un lenguaje específico conocido como HTML.

Es un documento adaptado para la Web y que habitualmente forma parte de un sitio web. Su característica principal son los hiperenlaces a otras páginas, siendo esto el fundamento de la Web.

Una página web está compuesta principalmente por información tal como: texto, imágenes, audio, video e hiperenlaces; además puede

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

contener o asociar datos de estilo para especificar cómo debe visualizarse, o aplicaciones embebidas para hacerla interactiva. [13]

Una página web necesita de un lugar donde alojarse para que al momento en que un usuario solicite información desde su navegador, la información que ésta contiene se cargue y aparezca en el ordenador. Es por esto, que los sitios web se encuentran alojados en un servidor web o host, que puede ser definido como un programa que se ejecuta continuamente en un computador, manteniéndose a la espera de peticiones de ejecución que le hará un cliente o un usuario de Internet. El servidor web se encarga de contestar a estas peticiones entregando como resultado una página web o información de todo tipo de acuerdo a los comandos solicitados.

El contenido de la página puede ser predeterminado o generado al momento de visualizarla o solicitarla a un servidor web. Según la forma de presentar contenido al usuario las páginas web se clasifican en estáticas y dinámicas. Las estáticas forman parte de épocas anteriores, puesto que son de contenido fijo y no son aptas a actualizaciones constantes. Las páginas dinámicas son generadas al momento de la visualización, esto se logra a través de lenguajes interpretados, generalmente JavaScript, PHP, JSP, etc y la aplicación encargada de visualizar el contenido es la que debe generarlo. Las páginas dinámicas solicitadas son creadas por una aplicación en el servidor web que alberga las mismas.

2.13 Niveles de una aplicación web

Una aplicación web suele estar conformada de tres niveles: interfaz de presentación, lógica de la aplicación y los datos, tal como se muestra en la Figura 2-3. [13]

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

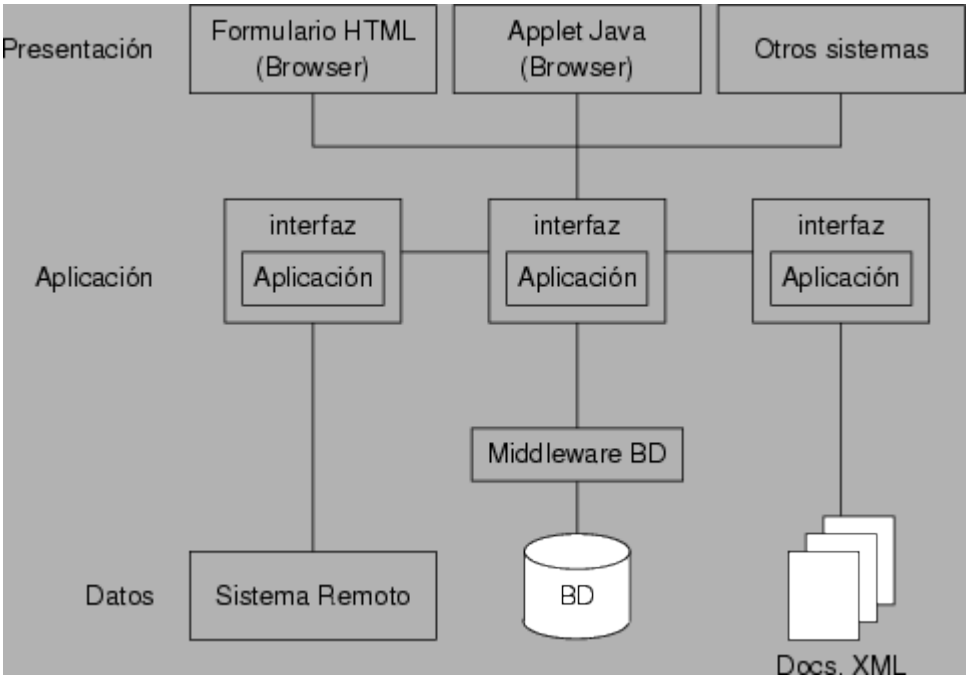


Figura 2-3: Niveles de una aplicación web (Tomado de [12])

- ***Presentación:*** está compuesto por páginas HTML que el usuario solicita a un servidor web y que visualiza en un cliente web, normalmente un navegador web.
- ***Lógica de aplicación:*** está compuesto por los módulos que implementan la lógica de la aplicación y que se ejecutan en un servidor de aplicaciones.
- ***Datos:*** está compuesto por los datos, gestionados por un sistema de gestión de bases de datos.

2.14 Aplicación Web

Una aplicación web es cualquier aplicación que es accedida vía web por una red como internet o una intranet cuya interface de usuario es accesible desde un cliente web, normalmente un navegador web. Esta compuesta de una estructura de directorios y algunos archivos requeridos, la estructura de directorios es la misma para todas las aplicaciones web.

En los inicios de Internet, los sitios web consistían de páginas estáticas, lo que generaba una interacción limitada con el usuario. Al

inicio de los 90, estas limitaciones fueron superadas cuando los servidores Web fueron reemplazados para permitir comunicaciones a través del desarrollo de fragmentos de código que eran ejecutados del lado del servidor. A partir de entonces las aplicaciones dejaron de ser estáticas y se permitió a usuarios normales interactuar con las aplicaciones por primera vez. [13]

Características

- Comunicación mediante HTTP sobre TCP/IP.
- Procesamiento en servidor.
- Acceso a bases de datos.
- Arquitectura por capas.
- Distintos tipos de usuarios.

2.15 Lenguajes de Programación orientadas a Aplicaciones Web

Los lenguajes de programación web han surgido según las necesidades de las plataformas, intentando facilitar el trabajo a los desarrolladores de aplicaciones. Se clasifican en lenguajes del lado cliente y lenguajes del lado servidor. [14]

Lenguajes del lado cliente

Son aquellos lenguajes que están relacionados directamente con el navegador y no necesitan un pre-tratamiento.

Lenguajes del lado servidor

Son aquellos lenguajes que se ejecutan por el propio servidor y son enviados al cliente en un formato claro para él.

2.16 Modelado de datos

Dentro de la estructura de los datos se encuentra lo que se conoce como modelo de datos, que no es más que una colección de herramientas conceptuales para describir los datos, las relaciones, la semántica y las restricciones de consistencia. En base de datos se

utilizan dos modelos: el modelo entidad-relación y el modelo relacional [15].

2.16.1 Modelo Entidad Relación

El modelo de datos entidad-relación (E-R) está basado en una percepción del mundo real que está formado por una colección de objetos básicos, denominados **entidades** y de relaciones entre ellos. Por ejemplo una cuenta, una persona o un vehículo puede ser considerado una entidad.

Las entidades están descritas en una base de datos a través de un conjunto de **atributos** por ejemplo número de placa, color, modelo pueden considerarse como atributos de la entidad vehículo. Un atributo especial puede ser utilizado para identificar unívocamente a una entidad.

Una **relación** es una asociación entre varias entidades. Por ejemplo una entidad persona puede ser asociada a la entidad vehículo.

2.16.2 Modelo Relacional

Este modelo utiliza un grupo de tablas para representar los datos y las relaciones entre ellos. Cada tabla está compuesta por varias columnas, y cada columna tiene un nombre único. El modelo relacional se ha establecido actualmente como el principal modelo de datos para las aplicaciones de procesamiento de datos.

2.17 HTTPS

HTTPS se diseñó con el fin de resistir a los ataques y ser más seguro que HTTP. Para lograr establecer una conexión HTTPS con el servidor web se debe crear un certificado de clave pública para el servidor web. Existen cuatro requerimientos que un servidor necesita brindar a una aplicación web:

- ***Autenticación:*** Cliente y servidor deben ser capaces de verificar que la persona que intenta ingresar es quien dice ser.
- ***Control de Acceso***: El acceso a recursos debe ser controlado. Únicamente los usuarios autorizados pueden acceder a un recurso deben hacerlo.
- ***Integridad:*** Los datos y la información no deben ser modificados fuera de la aplicación web.
- ***Confidencialidad:*** El acceso a la información es restringido a solo quien tiene los suficientes derechos.

  [16], [17], [18]

2.18 Servidor FTP

FTP (File Transfer Protocol) es un protocolo de red utilizado para la transferencia de archivos entre sistemas que se encuentran conectados a una red. Para acceder a un servidor FTP remoto se necesita un cliente FTP. Existen clientes FTP basados en web, es decir podemos ingresar desde el navegador, o también se puede utilizar aplicaciones como FileZilla, Free FTP, net2ftp, entre otros [19].

2.19 Servidor de Base de Datos

Un servidor de bases de datos es utilizado para almacenar, recuperar y administrar los datos de una base de datos. El servidor se encarga de la actualización de los datos, el acceso simultáneo de varios servidores o usuarios web y además garantiza la seguridad y la integridad de los datos. Los datos son los elementos a los que el usuarios están accediendo simultáneamente.

El software de servidores de bases de datos tiene herramientas para administrar las bases de datos. Entre las funciones de las bases de datos están la configuración del acceso de los usuarios y el respaldo de datos [20].

2.20 Cámara de video vigilancia

Una cámara IP es una unidad que emite imágenes a la red en forma digital. Como poseen su propio microrordenador estas pueden emitir video además de comprimirlo.

Tienen algunas funciones como el envío de correos electrónicos (e-mails) con imágenes, activación mediante detección de movimiento, activación a través de sensores o una alarma, control remoto de los movimientos de la cámara, gestionar el ancho de banda mediante la cantidad de CPS (cuadros por segundo) utilizados. Además permiten visualización en tiempo real independiente de la distancia que se encuentre a través de Internet. [21]

Una cámara IP comprime la información recopilada para que las imágenes que son digitalizadas tengan una resolución y velocidad buena. Entre los formatos de compresión más utilizados están MPEG4 y H.264. [22]

Para administrar la cámara se lo puede hacer con el software que tiene internamente las cámaras. Se debe ingresar la dirección IP o el nombre del servidor DNS a través del navegador.

La información recolectada por las cámaras IP es almacenada en su disco duro interno, en una tarjeta SD (si la cámara soporta), en disco externo o en un servidor mediante software de grabación que es suministrado por el fabricante de la cámara.

2.21 Arquitectura Modelo Vista Controlador

Es un patrón usado en ingeniería de software para separar la lógica de aplicación de la interface de usuario [23]. Este modelo permite separar la GUI (Graphical User Interface), de los datos y de la lógica apoyándose en tres componentes, a saber:

Modelo

Es la representación de los datos y de las reglas de negocio (mundo del problema). Sus funciones son:

- Contener el núcleo de la funcionalidad de la aplicación.
- Contener una representación de los datos que maneja el sistema, su lógica de negocio, y sus mecanismos de persistencia.
- Mantiene una independencia entre el Controlador y la Vista.

Vista

Permite mostrar la información del modelo en un formato adecuado que permita que se realice la interacción. Cumple las siguientes funciones:

- Es la presentación del Modelo.
- Permite acceder al Modelo pero nunca cambiar su estado.
- Permite ser notificada cuando hay un cambio de estado en el Modelo.
- Compone la información que se envía al cliente y los mecanismos interacción con éste.

Controlador

Responde a los eventos provocados por el usuario (dar un clic, digitar un texto, etc) que implica cambios en el modelo y la vista, brindando una correcta gestión a las entradas del usuario. Entre sus funciones destacan:

- Actúa como intermediario entre el Modelo y la Vista, gestionando el flujo de información entre ellos y las transformaciones para adaptar los datos a las necesidades de cada uno.

- Reacciona a la petición del Cliente, ejecutando la acción adecuada y creando el modelo pertinente

El flujo que generalmente se sigue se muestra en la Figura 2-4:

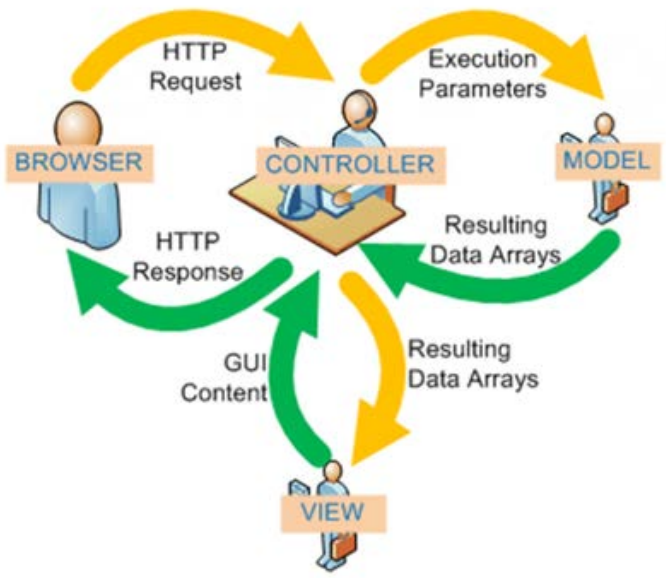


Figura 2-4: Flujo Modelo Vista Controlador. (Tomado de [23])

Los pasos seguidos en el flujo son los siguientes:

1. El usuario interactúa con la interface de alguna manera (por ejemplo, el usuario pulsa un botón, enlace, etc.)
2. El controlador recibe la notificación de la acción solicitada por el usuario. El controlador gestiona el evento que llega, generalmente a través de un gestor de eventos (handler o callback).
3. El controlador accede al modelo, y lo actualiza, posiblemente modificándolo de acuerdo a la acción solicitada por el usuario.
4. El controlador confía a los objetos de la vista la tarea de desplegar la interface de usuario. La vista obtiene sus datos del modelo para generar la interface apropiada para el usuario donde se refleja los cambios en el modelo.
5. La interface de usuario espera nuevas interacciones del usuario, comenzando el ciclo nuevamente.

CAPÍTULO 3

ANÁLISIS DE REQUERIMIENTOS Y SEGURIDAD DE LA RED

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 3 ANÁLISIS DE REQUERIMIENTOS Y SEGURIDAD DE LA RED.

En este capítulo se hace una descripción general de la red de ETAPA EP, que es el medio por el cual se transmitirán los datos de la central de alarma al servidor que se encuentra en el DataCenter, y una descripción de la red LAN que es la que establecerá la comunicación con el servidor. Además se realiza un análisis de la seguridad del medio de comunicación, de la “aplicación cliente” y de la “aplicación servidor”.

Análisis de requerimientos de red

3.1 Descripción de la red de ETAPA EP

La red de la Empresa Pública Municipal de Telecomunicaciones, Agua Potable y Saneamiento - ETAPA EP dispone de una red de transmisiones, encargada de interconectar los distintos nodos de acceso que están emplazados en varios sectores de la ciudad, esta red está basada en conexiones físicas mediante fibra óptica y routers de alta capacidad con interfaces de conexión GigaEthernet o 10GigaEthernet, con los protocolos IP/MPLS (Internet Protocol / Multi Protocol Label Switching), que garantizan calidad de servicio.

La red de acceso, que es el segmento que interconecta los nodos de acceso con el usuario final, consta básicamente de redes físicas basadas en par trenzado de cobre sobre la cual se utiliza tecnología ADSL2+ (Asimetric Digital Suscriber Line), VDSL2 (Very High Data Rate Digital Suscriber Line) y se usa también fibra óptica con tecnología GPON (Gigabit Pasive Optical Network).

En las inmediaciones del cliente se utilizan equipos terminales de Acceso que se interconectan a la red pública ya sea mediante cobre (xDSL) o fibra óptica (GPON) y proveen conexiones Ethernet para interconectar los equipos del cliente.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

La red de transporte se conecta con los puntos de distribución de servicios, el cual incluye el núcleo de distribución de servicios de internet ISP (Internet Service Provider). Este cuenta con servidores, equipos de seguridad, control de acceso y almacenamiento (cache), el SOFTSWITCH que maneja los servicios de telefonía, el DataCenter que brinda coubicación y servicios de alojamiento de datos y contenidos para empresas. En la Figura 3-1 se describe de manera general la red de ETAPA EP.

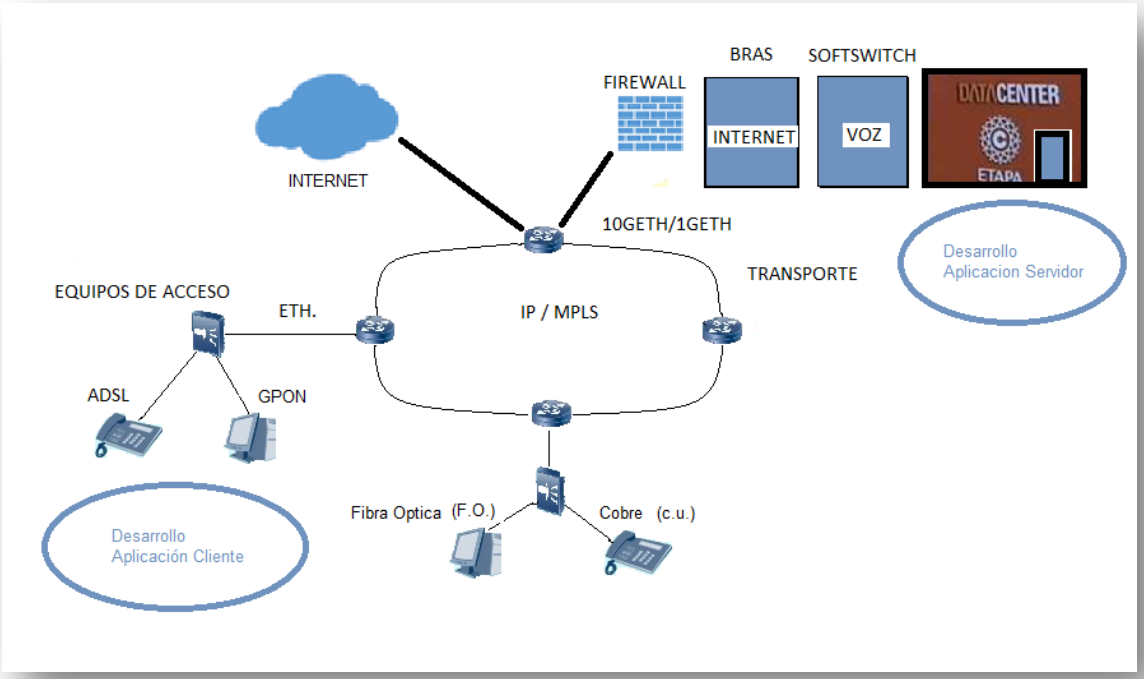


Figura 3-1: Descripción de la red de ETAPA EP

3.2 Descripción de la red de la aplicación cliente y aplicación servidor

La manera en la que se comunica la "aplicación cliente" con la "aplicación servidor" es mediante la arquitectura cliente-servidor, utilizando TCP/IP. El canal de datos TCP/IP puede ser el servicio de Internet que se contrata con un ISP.

En la red LAN, se utiliza los siguientes protocolos: El protocolo Ethernet 10Base-T a nivel de capa física y enlace de datos. En la

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

capa de red se establece el protocolo IP y el enrutamiento es realizado por el modem del domicilio. A nivel de capa de transporte se maneja el protocolo TCP y adicionalmente en las capas de sesión, presentación y aplicación se necesita de un protocolo de comunicación que pueda establecer conexión con el Servidor.

En la “aplicación servidor” se utilizan los protocolos http y ftp a nivel de capa de aplicación. Estos permiten establecer la comunicación con los servidores ftp, web y de base de datos.

Análisis de la seguridad en la red

3.3 Seguridad en el medio de transmisión

La seguridad en el medio de transmisión implica la protección de los datos cuando la comunicación desde la red LAN hacia el servidor ubicado en el DataCenter es establecida. Los datos deben ser cifrados, de forma que terceros no puedan entenderlos y para ello se puede utilizar el protocolo HTTPS, el cual permite transferir datos cifrados a través del protocolo SSL (Capa de Sockets Seguros) o TLS (Seguridad de Capa de Transporte).

3.4 Seguridad en la red de la Aplicación Cliente

La autenticación mediante usuario y contraseña es lo mínimo requerido para proteger los datos en una red, en donde el usuario se identifica previamente.

Para la seguridad en el modem debe tener autenticación por medio de usuario y contraseña, para evitar el ingreso a la página de configuración del modem. Además los dispositivos que se encuentran vinculados al puerto LAN mediante el estándar IEEE 802.1x deben contar con autenticación.

3.6 Seguridad en la red de la Aplicación Servidor

Los servidores pueden estar expuesto a ataques externos y para protegerse de estos, se debe contar con los equipos adecuados para autenticación. Además se debe contar con firewalls que bloqueen el acceso a ciertos puertos y para proteger datos que son sensibles en las aplicaciones web se debe utilizar el protocolo https.

3.7 Mitigación de riesgos en la aplicación cliente

Contraseña en la Central de Alarma: El primer mecanismo para identificar al servidor y ser identificado por el mismo es la autenticación. Para la autenticación con el servidor se establece el método de ingreso de contraseña. Cada cliente es configurado con un código que se encuentra registrado en el servidor, de esta manera el cliente envía un paquete de datos con el código y la contraseña. Si los datos son correctos el servidor responde al cliente indicándole que puede ingresar al sistema.

Establecimiento de conexión desde la Central de Alarmas: Mediante el protocolo TCP se crea un canal virtual denominado Socket. Existe varios parámetros como: IP local, IP remoto, puerto local, puerto remoto, que la Central de Alarma debe interpretar para que solo paquetes que cumplan con estos parámetros sean interpretados al momento de establecer la conexión entre cliente y servidor, el proceso se muestra en la Figura 3-1.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

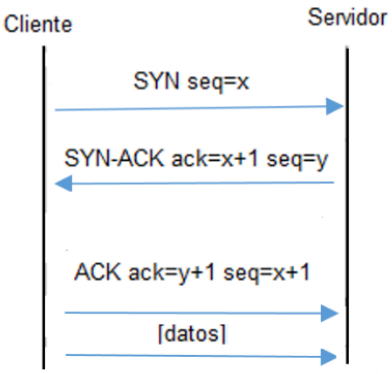


Figura 3-1: Proceso de establecimiento de conexión entre cliente y servidor

Usuario y contraseña de la cámara IP: La cámara IP debe contar con autenticación por usuario y contraseña, debido a que desde Internet solo debe ingresar la persona autorizada.

Nivel de Acceso: El web server de la cámara IP posee niveles de seguridad en el acceso que deben configurarse para tener una mayor protección, como son administrador, operador y visitante.

3.8 Mitigación de riesgos en la aplicación servidor

Firewall: El uso de firewalls es importante para bloquear el acceso a cierto tipo de información en el servidor, habilitando o deshabilitando puertos. Por ejemplo para que una aplicación web sea accesible al exterior se debe habitar el puerto 80 y/o 8080 (http).

Autenticación en el servidor: El servidor debe configurarse de forma que solo el administrador tenga acceso a los archivos de configuración internos, para ello se utiliza autenticación tanto para acceso de forma local como remota.

Certificados de seguridad SSL: La creación y configuración de certificados digitales en el servidor permite el acceso seguro a la aplicación web que contiene información valiosa.

Control de Acceso: Se debe controlar el acceso al servidor cuando se usa el servicio de transferencia de archivos (FTP).

CAPÍTULO 4

DESARROLLO APLICACIÓN CLIENTE

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 4 DESARROLLO APLICACIÓN CLIENTE

4.1 Análisis de la situación actual

Para ofrecer una alternativa a los sistemas de seguridad electrónica, se realizó mediante la ayuda de encuestas, un análisis que reflejará una idea de la situación actual de los sistemas de seguridad, las empresas que dan este servicio, los servicios que disponen, etc.

La encuesta fue realizada a una muestra de 300 clientes de ETAPA EP, y a continuación se analizan las respuestas de cada pregunta:

¿Cuenta con servicio de Seguridad Electrónica en su hogar?

El resultado se muestra mediante el gráfico de la Figura 4-1.

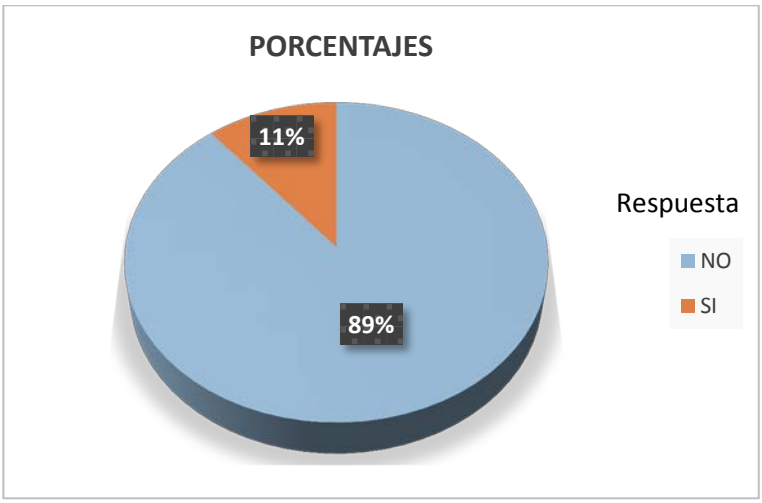


Figura 4-1: Porcentaje de clientes que cuentan con servicio de seguridad electrónica en su hogar.

Con esta pregunta se puede llegar a estimar el número de usuarios que poseen sistema de seguridad electrónica en su hogar. Siendo solo el 11% de los encuestados que cuentan con este servicio, el cual es un porcentaje bajo de clientes en el mercado, con lo cual se deduce que los sistemas de seguridad electrónica no son tan

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

utilizados, ni difundidos. Por esta razón se convierten en sistemas de proyección hacia el futuro.

¿Con cuál de las siguientes empresas tiene contratado el servicio?

El resultado se muestra mediante un gráfico en la Figura 4-2.

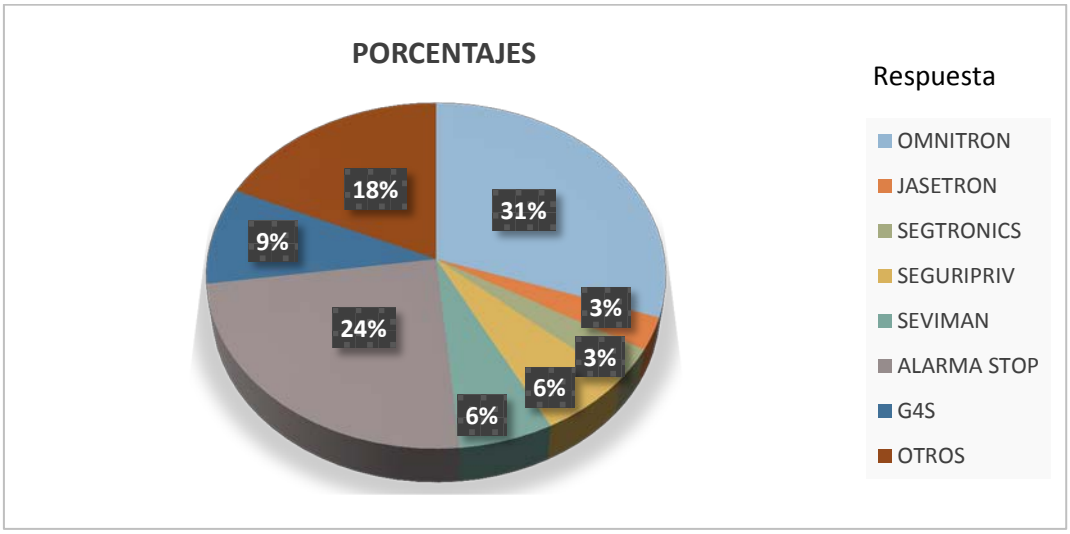


Figura 4-2: Distribución porcentual de clientes en las diferentes empresas de seguridad.

Con esta pregunta se determina, las empresas que ofrecen el servicio y captan más clientes, entre estas se tiene a OMNITRON, ALARM STOP, G4S, las cuales son empresas que ofrecen servicios como: alarma, monitoreo, circuito cerrado de video, respuesta armada, etc.

¿Qué servicio tiene contratado?

El resultado se muestra mediante un gráfico en la Figura 4-3.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

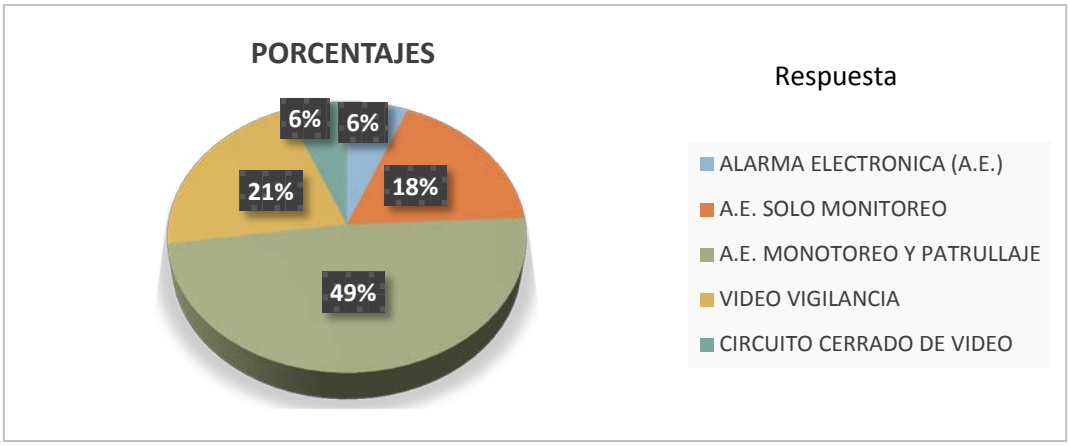


Figura 4-3: Servicios de seguridad electrónica contratados

Se busca determinar cuál servicio es el más contratado por los usuarios de sistemas de seguridad, siendo el monitoreo y patrullaje el más solicitado por los clientes, con este servicio se ofrece la instalación, el control con el monitoreo adecuado y la debida atención a las alarmas con patrullajes continuos.

¿Le gustaría tener servicio de Video Vigilancia desde su Smartphone, Tablet o Computador?

El resultado se muestra mediante un gráfico en la Figura 4-4.

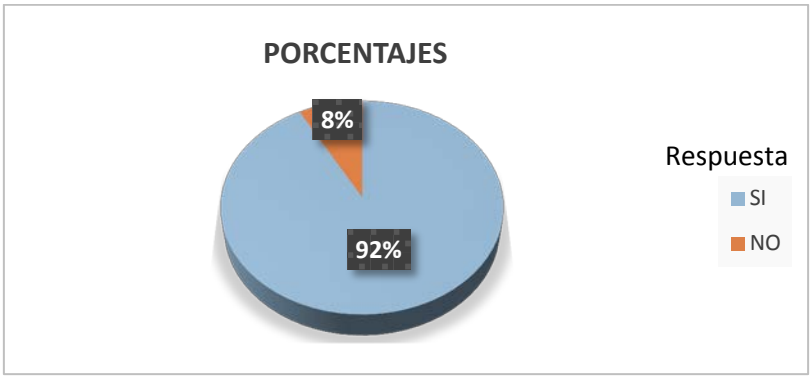


Figura 4-4: Preferencia de las personas hacia un nuevo servicio

La pregunta muestra la aceptación de los usuarios al monitoreo de forma remota a través de un Smartphone, Tablet o computador, como alternativa de servicio adicional para incorporar a los sistemas de seguridad electrónica.

Como resultado de las encuestas realizadas se toma como referencia a la empresa OMNITRON, para establecer el kit básico de una alarma, que permitirá desarrollar la “aplicación cliente” a emplearse en el sistema de seguridad electrónico. [24]

A continuación se nombra los componentes básicos de un kit de alarma

- Panel PC585ZD:
- Teclado PC1555RKZ:
- Batería
- Transformador
- Sirena
- Gabinete
- Sensor de movimiento
- Sensor magnético

4.2 Funcionamiento y diseño de la aplicación cliente

4.2.1 Definición general de la solución

Bajo el análisis de la situación actual de los sistemas de seguridad residenciales (sección 4.1) se determinó que la “aplicación cliente” más apropiada para el sistema se basa en un sistema centralizado a través de la implementación de una cámara de video y central de alarma, la cual se encarga de gestionar las señales de los sensores y enviarlas a través de la red IP a la “aplicación servidor”, además consta de sensores, dispositivos que permitan la conexión a la red IP, etc.

La “aplicación cliente” se comunica a través de la red de ETAPA EP con la “aplicación servidor”, como se muestra en la Figura 4-5, para ello se utiliza el modem instalado en los domicilios.

Figura 4-5: Esquema de comunicación entre la aplicación cliente y la aplicación servidor

Dentro de la “aplicación cliente” se consideran dos subsistemas denominados central de alarma y video-vigilancia.

Central de alarma: Se encarga de gestionar el estado de los sensores y comunicarse con la “aplicación servidor” para monitorear el estado de los sensores del domicilio. La central de alarma se subdivide en módulos con el fin de facilitar su desarrollo, de manera que cada módulo puede ser desarrollado por separado y actualizado según sus requerimientos.

Cada uno de los módulos a su vez interactúa con los siguientes periféricos: sensores, batería, sirena, módulo GSM, trasformador, módulo Ethernet.

En la figura 4.6 se muestra el esquema de la central de alarma con sus respectivos módulos y periféricos.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

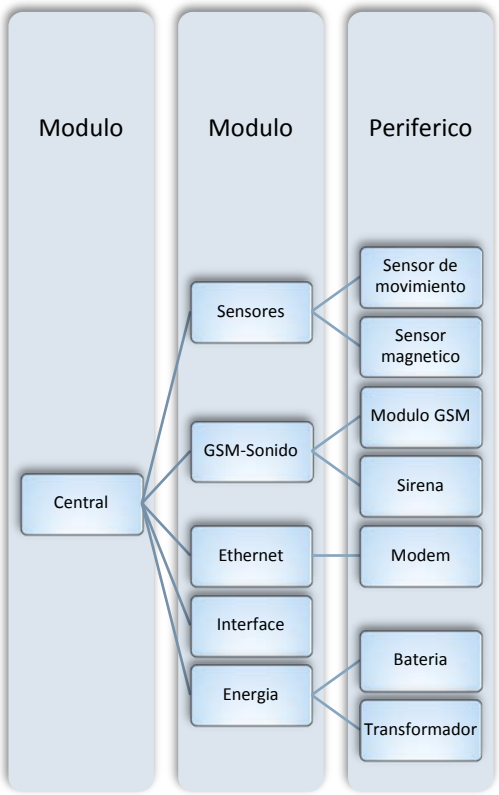


Figura 4-6: Esquema de la Central de alarma con sus respectivos módulos y periférico.

4.2.2 Video-vigilancia

Se encarga del almacenamiento en el servidor y de la monitorización de las cámaras IP. La cámara IP emite las imágenes directamente a la red sea LAN o WAN, además de comprimirlas antes de enviarlas a través de la red. Esta debe comunicarse con la "aplicación servidor" para tener almacenamiento de imágenes en caso que haya detección de movimiento. Para ello se la debe configurar con la dirección IP de la "aplicación servidor", ver Anexo C.

Video-Vigilancia consta de:

- ***Almacenamiento en el Servidor:*** Debido a que la cámara posee la funcionalidad de detección de movimiento, en el momento que se produzca un movimiento, se capturan las

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

imágenes del evento durante un intervalo de tiempo y se las almacenan en el servidor.

- ***Monitorización de las cámaras:*** La cámara IP tiene funciones como el envío de correos electrónicos (e-mails) con imágenes, activación mediante detección de movimiento, activación a través de sensores o una alarma, control remoto de los movimientos de la cámara, gestión del ancho de banda, además de permitir la visualización en tiempo real a través de la red LAN del cliente o de una red WAN haciendo que sea independiente de la distancia que se encuentre. Para su configuración a través de una red WAN se debe utilizar un DDNS (Dynamic Domain Name System) y habilitar los puertos en el modem del usuario, ver Anexo D.

4.2.3 Selección de protocolos y medios de transmisión.

La "aplicación cliente" está compuesta por subsistemas y estos a su vez por módulos. Para comunicar cada elemento se necesita definir protocolos y medios de transmisión. En la Tabla 4-1 se indica los protocolos y medios utilizados entre cada uno de los elementos.

Subsistema	Servidor	Protocolo	Medio de Transmisión
Central Alarma	Aplicación servidor	TCP/IP	Cable UTP
Video-vigilancia	Aplicación servidor	TCP/IP, FTP	Cable UTP
Módulo	**Módulo**	**Protocolo**	**Medio de Transmisión**
Interface	Central	PP	Cable plano 10 hilos
Gestión Energía	Central	N/A	Cable plano 10 hilos
Sensores	Central	N/A	Cable plano 10 hilos
Ethernet	Central	SPI	Cable plano 10 hilos
GSM Sonido	Central	AT	Cable plano 10 hilos
Periférico	**Módulo**	**Protocolo**	**Medio de Transmisión**
Sensores	Sensores	N/A	Gemelo # 16, UTP 2 pares
Batería	Gestión Energía	N/A	Gemelo # 12

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Sirena	GSM Sonido	N/A	Gemelo# 12
GSM	GSM Sonido	AT	UTP 2 pares

Tabla 4-1: Protocolos y medios de transmisión utilizados.

Protocolos: Cada uno de los protocolos y medios de trasmisión se seleccionaron de acuerdo a las condiciones de los equipos y requerimientos de la solución.

TCP/IP (Transmission Control Protocol): es el protocolo de comunicaciones utilizado por las redes de ETAPA EP. Por lo tanto la central de alarma y video-vigilancia tiene que entender este protocolo para comunicarse con la "aplicación servidor".

FTP (File Transfer Protocol): es el protocolo que la cámara de video utiliza para transmitir imágenes. El cual viene incorporado dentro del software de la cámara.

SPI (Serial Peripheral Interface): es un protocolo de comunicación síncrono, que viene incorporado en el integrado ENC28J60 y en microcontroladores, muy utilizado para la comunicación de los mismos. [25]

AT (Attention): es un protocolo que viene incorporado en el módulo GSM para comunicarse con microcontroladores que cuente con módulos USART.

RS232 (Recommended Standard 232): es un protocolo incorporado en microcontroladores. Su elección se debe a la flexibilidad que presenta al momento de desarrollar otros protocolos basándose en el mismo.

PP es un protocolo propio, desarrollado para el prototipo.

Medios de Transmisión: Por los medios de transmisión circulan datos y potencia para alimentar a los periféricos. Los medios de transmisión utilizados son:

- *Cable UTP:* cable de 4 pares de cobre, los cuales se utilizan en redes TCP/IP.
- *Cable plano 10 hilos:* su selección de debe a la facilidad de adaptarse a los conectores utilizados en cada módulo.
- *Cable UTP 2 pares:* seleccionado por el número de hilos que se requiere para poner en funcionamiento el módulo GSM y su comunicación.

PP implementa un conjunto de comandos que cumplen las siguientes funciones:

- Comando Alarma: Activar o desactivar los sensores de una zona determinada.
- Comando Intruso: Intruso detectado.
- Comando ConfigSensor: Configurar sensores en las zonas.
- Comando ConfigClave: Configuración de la clave de usuario.
- Comando Recibido: Acuse de recibo.
- Comando Estado: Monitoreo de estado.
- Comando Pánico: Mensaje de pánico.
- Comando Conexión: Monitoreo de la conexión.

El conjunto de bytes del protocolo PP se organiza de la siguiente manera:

- El byte de inicio es cero e indica el inicio del paquete
- 4 bytes de código que pueden ser seleccionados del 0000 al 9999
- El byte de comando puede tomar valores del 1 al 8 según la operación que se desea realizar
- El byte 7 es el primer dato que se envía, este puede ser un número de sensor o una acción
- 5 bytes adicionales que llevan datos
- El byte de fin de paquete determinado por 255

- El byte suma encargado de llevar la suma de todos los bytes con el fin de determinar si algún bit ha sido alterado en el transcurso.

En la Tabla 4-2 se detallan los comandos y parte de los datos que se pueden enviar

#	Comando	Dato1	Dato2	Dato3	Dato4	Dato5	Dato6
1	Alarma	10 0ff, 11 On	# Zona				
2	Intruso	# Sensor					
3	ConfigSensor	10 0ff, 11 On	# Sensor	# Zona			
4	ConfigClave	Acción	Clave1	Clave2	Clave3	Clave4	
5	Recibido						
6	Estado						
7	Pánico						
8	Conexión						

Tabla 4-2: Detalle de Comandos del protocolo propio (PP)

Ejemplo de uso de PP (Tabla 4-3): Paquete que indica que un cliente con código 1111 ha presionado el botón de pánico.

Byte #1	Byte #2	Byte #3	Byte #4	Byte #5	Byte #6	Byte #7	Byte #7
INICIO	Código	Código	Código	Código	Comando	FIN	SUMA
0	1	1	1	1	7	255	11

abla 4-3: Ejemplo de paquete PP

4.2.4 Módulo central

Es el cerebro del sistema, lleva incorporado un microcontrolador que soporta la programación del sistema según las funciones que se definen a continuación.

- **Gestiona el protocolo PP:** Permite la comunicación del módulo central con el panel de usuario. Permite la configuración de sensores en determinada área del domicilio o en todo, a esta división se la denomina zona, de

modo que el sistema admite la configuración de hasta 3 zonas.

- **Gestiona la comunicación con el servidor:** Configura un canal de comunicación a través de sockets, para ello se utiliza una librería de libstock llamada Net_Ethernet_28j60. Cabe indicar que a cada cliente del sistema se le asigna un código de cuatro dígitos para reconocer a quien pertenece la central de alarma y poder comunicarse con la aplicación servidor.
- **Gestiona el respaldo de energía:** Dado que la fuente principal de voltaje de la central de alarma es la red eléctrica del domicilio, esta es medida periódicamente para determinar si la batería pasa a ser fuente principal o continua de manera normal. Además debido a que el microcontrolador de la central de alarma es alimentado por la batería, el nivel de voltaje de la misma es medida para establecer si se continúa usando o se carga para su posterior uso.
- **Gestiona el respaldo GSM:** Determina si se pierde la comunicación con el servidor, de tal forma que utiliza la red GSM como medio de comunicación de respaldo en caso de la ocurrencia de un evento.
- **Gestiona la comunicación entre módulos:** Cuenta con varios puertos IDC para comunicarse con todos los módulos, permitiendo la comunicación entre ellos.

Su base es el PIC18F45K22 que cumple con las exigencias del sistema, es decir cumple con cada una de las funciones antes descritas mediante el uso de USART, ADC, SPI, TIMER, etc.

4.2.5 Módulo Energía

Tiene como función principal dotar a la central de alarma de los niveles de voltaje adecuados, además de medir los niveles de

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

voltaje y controlar la energía proveniente de la red eléctrica y de la batería para la gestión en el módulo central.

El modulo está conformado con los siguientes conectores:

- Dos para la conexión de la batería
- Dos para alimentación de la red eléctrica
- Cinco para alimentar el resto de módulos de la central de alarma de: 12, 12, 5, 3.3 y 0 V.
- Cinco para monitoreo y control del mismo, distribuidos de la siguiente manera 2 pines para controlar el nivel de tensión de la red eléctrica y la batería, 3 pines para activar o desactivar el paso de corriente hacia o desde la batería.

4.2.6 Módulo sensores

Sirve como interface entre los sensores y la central de alarma. Soporta la conexión de hasta 7 sensores, ofrece conexión a 12V y niveles lógicos a 5V.

4.2.7 Módulo Ethernet

Se encarga de la comunicación entre la “aplicación servidor” y la central de alarma. El núcleo de este módulo es el integrado ENC28J60 que permite convertir el protocolo SPI a Ethernet y viceversa.

4.2.8 Módulo Interface

Tiene la función de interactuar con el usuario, el mismo que está conformado por el panel de usuario y convertidor. Al conjunto pantalla LCD y teclado matricial 4x4 se lo denominado panel de usuario y al circuito que cambia el estándar del conector, de IDC a RJ45 y viceversa se lo denominado convertidor. Mediante el panel de usuario se visualiza el estado actual de la central de alarma y se

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

recoge los datos ingresados, como por ejemplo al presionar la letra “A” se activan los sensores.

El panel está controlado por el microcontrolador PIC18F14K22, funciona con una alimentación de 5V y tiene un puerto RJ45 para comunicación con el modulo central.

Se usa mayormente como soporte en caso de problemas de comunicación con la “aplicación servidor”.

4.2.9 Módulo GSM-Sonido

Tiene 3 funciones principales:

- Comunicarse con el módulo GSM mediante 4 pines, los mismos que son 5V, GND, Tx y Rx.
- Activar o desactivar el sonido de la Sirena a través de un Relé.
- Monitorear el estado del enlace de la central de alarma y la aplicación servidor por medio de la visualización de 3 Leds.

4.2.10 Esquema de conexión de la central de alarma

Para cada módulo se realizó su diseño electrónico, los mismos que se muestran en el Anexo H.

A continuación se muestran en la figura 4-7 las conexión entre cada módulo de la central de alarma a través de sus diferentes conectores y protocolos.

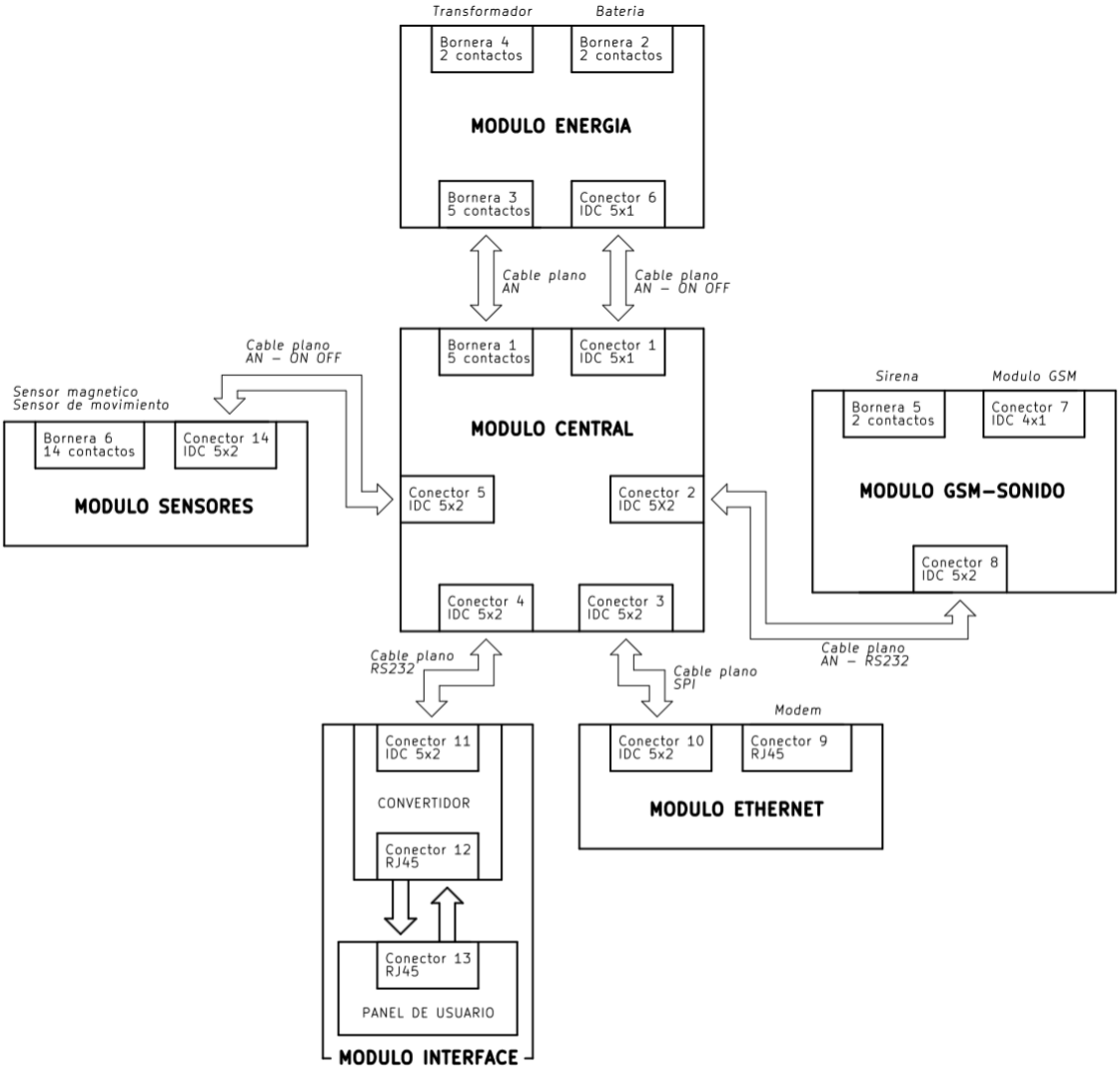


Figura 4-7: Esquema de conexión de la Central de alarma

Por ejemplo el modulo sensores se conecta con el modulo central a través de conectores IDC 5x2 y cable plano, además las señales que trasmiten son analógicas (AN, voltaje de alimentación) y ON OFF (valor lógico 1 o 0).

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 5

DESARROLLO APLICACIÓN SERVIDOR

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 5 DESARROLLO APLICACIÓN SERVIDOR

5.1 Desarrollo aplicación servidor

En este capítulo se analizan los requerimientos necesarios en la parte de software tales como: sistema operativo, lenguajes de programación del lado servidor y cliente que darán soporte a las aplicaciones encargadas de la gestión y comunicación con el sistema de seguridad. Un esquema general de éste desarrollo se muestra en la Figura 5-1.

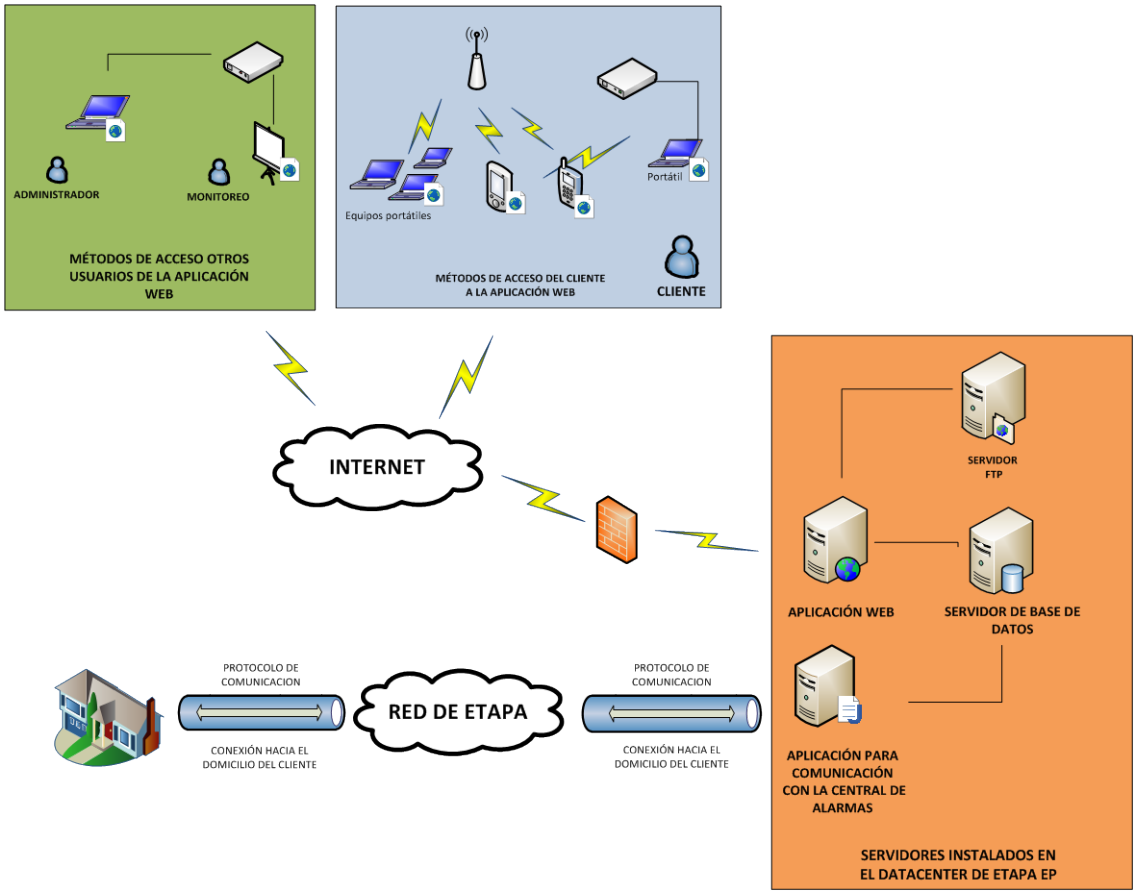


Figura 5-1: Esquema general "Desarrollo Aplicación Servidor"

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Es necesario del desarrollo de una aplicación web que se encargue de la gestión del sistema de seguridad, manejo e interpretación de los datos generados por los dispositivos electrónicos, almacenamiento de video e información de los usuarios que conforman el sistema. Además, es necesario el desarrollo de una aplicación que se encargue de la comunicación con la central de alarmas instalada en el domicilio

Este proyecto utiliza software libre en el sistema operativo, software de desarrollo, APIs y servidores. El software libre brinda la facilidad en adquirir información compartida en internet y facilidad para personalización del software de acuerdo a las necesidades del usuario.

5.2 Selección del Sistema Operativo para el Servidor

Existen varias distribuciones GNU/Linux, cada una con sus ventajas y desventajas. La capacidad de elección para una distribución es amplia, sin embargo, las opciones son algo más limitadas en el campo de los servidores. Debido a la gran cantidad de distribuciones existentes, se consideró el artículo publicado por Linux.com “Las 7 mejores distribuciones del sistema operativo Linux del 2013”. [26] Dentro del campo de servidores se han considerado las siguientes cuatro:

- **Debian:** Es la más antigua de las distribuciones y la única en la que no existe una compañía comercializándolo. Es un sistema operativo GNU basado en software libre, mantenido totalmente por voluntarios vinculados por el contrato social Debian.

- **Ubuntu:** Es la distribución con más acogida en los últimos años, al contar cada vez con más usuarios y la que más

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

rápido se ha adaptado a las necesidades de los mismos y cuenta con su versión en el servidor.

- **Red Hat Enterprise:** RHEL **(**Red Hat Enterprise Linux) es quizá la distribución de Linux más conocida y muy popular en el campo de servidores. Ha contribuido con un gran número de aplicaciones para la comunidad de código abierto. El acceso a soporte y actualizaciones de seguridad requiere que los clientes paguen un honorario por estos derechos.

- **CentOS:** CentOS (Community Enterprise Operating System) es una ramificación a nivel binario de la distribución RHEL, compilado por voluntarios a partir del código fuente liberado por RHEL. CentOS es robusto, estable, fácil de instalar y utilizar.

Debido que la "aplicación servidor" está orientada a la utilización software libre, se tiene como mejor opción a CentOS, ya que es un sistema operativo gratuito y de software libre, su distribución está basada en RHEL una distribución popular en el campo de servidores y cuenta con una compatibilidad del 100% a nivel binario.

5.2.1 CentOS

Al ser CentOS es una versión libre de RHEL, no se debe cancelar valores por el acceso a actualizaciones de seguridad. Esto es posible debido a la licencia libre bajo la cual se libera el código de RHEL. CentOS es utilizado comúnmente como un sistema operativo servidor a nivel empresarial.

5.2.1.1 Requisitos del Sistema

Recomendación de Hardware para operar:

- Memoria RAM: 64 MB (mínimo).

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

- Espacio en Disco Duro: 1024 MB (mínimo) - 2 GB (recomendado).
- Procesador: ver sección 5.2.1.2

5.3 Servidor FTP

Debido a que la cámara IP no puede grabar video en el servidor y esta usa el protocolo FTP para transferir archivos hacia un servidor FTP. Se decidió realizar un script que genere video a partir de la secuencia de imágenes almacenadas en el servidor, durante la detección de movimiento. Se escogió el servidor *vsftpd*, que cuenta con licencia GPL y existe en los sistemas basados en Unix.

5.4 Arquitectura de Software

La arquitectura de Software del sistema está basada en el patrón de arquitectura Modelo Vista Controlador (MVC). El propósito principal es establecer una separación clara entre la interface de usuario que presenta la aplicación y la lógica de negocio manejada por la aplicación. Estas dos capas interactúan por medio del controlador que se encarga de responder a las acciones de la vista y solicitar peticiones al modelo. Este modelo presenta ventajas al desarrollador del software y al sistema ya que permite flexibilidad en cambios, modularidad, escalabilidad, actualizaciones en todas sus capas; es decir al realizar un cambio en una de las capas, el resto de sus capas no se verán afectadas. Este modelo es adaptable a la arquitectura en capas del sistema a ser desarrollado. [23]

54.1 MVC: Capa Modelo

La Capa Modelo es en donde se almacena toda la información del sistema, por ejemplo el estado de los sensores, configuración del sistema, información de los usuarios, dispositivos, etc. En esta capa se establecen las relaciones entre la información.

La información en este modelo se almacena en un SGBD. En este proyecto se ha decidido usar MySQL.

MySQL es una base de datos objeto-relacional de software libre y de código abierto. Su gran aceptación se debe, en parte, a gran variedad de librerías y herramientas que permiten su uso a través de distintos lenguajes de programación.

Esta base de datos es considerada como la más rápida y robusta tanto para volúmenes de datos grandes como pequeños, aunque está rapidez es a costa de no implementar ciertos aspectos del SQL.

Para la implementación de la base de datos se establecieron las funcionalidades permitidas para cada uno de los usuarios que conforman el sistema. En el sistema de seguridad se consideran tres tipos de usuarios que se describen a continuación:

Cliente: usuario al que se le configura el sistema de alarma y es propietario de la misma.

Monitoreo: encargado de supervisar el estado de los sensores que conforman el sistema de alarmas y video vigilancia de los diferentes clientes.

Administrador: encargado de la gestión de usuarios y configuración del sistema de alarma.

Se diseñó diagramas en base de las funcionalidades de usuario y un modelo lógico para el sistema de Bases de Datos, los cuales se observan en el Anexo B.

5.4.1.1 Arquitectura MySQL

MySQL consiste en un demonio servidor ***mysqld*** que es ejecutado en segundo plano a la espera de las peticiones realizadas por los clientes. Estas peticiones son procesadas por el motor de Base de Datos MySQL el que implementa

tecnología de multithread. Multithread se refiere a que MySQL puede ocuparse de muchas tareas y peticiones al mismo tiempo sin necesidad de terminar los procesos o consultas de unos clientes para atender los de otros.

5.4.1.2 Conexión MySQL con Java

Para la conexión entre las aplicaciones del sistema y la base de datos se utiliza JDBC (Java Database Connectivity). JDBC es una API pura de Java que suministra una cantidad considerable de clases e interfaces que permiten al desarrollador realizar operaciones sobre una base de datos. Estas operaciones incluyen la conexión a la base de datos, ejecución de comandos SQL, y extracción de datos.

JDBC es un middleware entre el lenguaje Java y una base de datos. Fundamentalmente, JDBC es una especificación que provee un conjunto completo de interfaces que permiten el acceso a una base de datos a través de una API estándar.

5.4.2 MVC: Capa Controlador

La Capa Controlador, es la encargada de la administración y coordinación de las peticiones del usuario hacia la capa de modelo, tiene la capacidad de actualizar los datos enviados del usuario y restringir acceso a la lógica del negocio. Dicho de otro modo, controla el flujo de información entre la capa Modelo y la capa Vista con la capacidad de ejecutar las peticiones hacia el modelo y las respuestas hacia la vista.

Se ha decidido utilizar como controlador un servidor de aplicaciones puesto que es el encargado de proporcionar servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones gestiona la mayor parte de las funciones de lógica de negocio y de acceso a los datos de la aplicación.

5.4.2.1 Servidor de Aplicaciones Java EE

Los servidores de aplicaciones desarrollados bajo el lenguaje JAVA mantienen la misma línea de administración de aplicaciones WEB, con posibilidades diversas en cuanto a capacidades de Clustering, manejo de conexiones de bases de datos, persistencia y cumplimiento del estándar JAVA EE. A continuación la Tabla 5-1 presenta el estudio de los servidores de aplicaciones propuestos y sus arquitecturas en particular.

Servidor de Aplicaciones	Proveedor	Licencia	Soporte disponible por el proveedor	Versión Java
GlassFish Server 3.01	Oracle	Comercial	Si	HotSpot 6/7
GlassFish Server Open Source Edition 3.x	Oracle	GPL + CDDL	No	HotSpot 6/7
WebSphere Application Server 8.x	IBM	Comercial	Si	IBM JVM 7
WebSphere Application Server Community Edition 3.0	IBM	IBM International License Agreement for Non-Warranted Programs	Si	IBM JVM 7
WebLogic Server 12.1.1	Oracle	Comercial / Libre	Si	HotSpot 6/7
JBoss Application Server 7.x	RedHat	LGPL	No	HotSpot 6

Tabla 5-1: Principales Servidores de Aplicaciones JavaEE

Lo que se busca es un servidor que soporte Java EE 6. Cuatro de los servidores que se muestran en la Tabla 5-1 están entre las posibles opciones de selección, aunque son discutibles desde el

punto de vista de licencia. Tanto JBoss y Oracle GlassFish Enterprise Server tienen una licencia comercial, pero aún confían en los productos de software libre y la versión con licencia sólo es relevante si se desea tener soporte. La Tabla 5-2 lista los servidores que no ofrecen soporte del proveedor.

Servidor de Aplicaciones	Proveedor	Licencia	Soporte disponible por el proveedor	Versión Java	Servidor de Aplicaciones
GlassFish Server 3.01	Oracle	Comercial	FP	Si	HotSpot 6/7
JBoss Enterprise Application Platform 6	RedHat	LGPL / Comercial	FP	Si	HotSpot 6

Tabla 5-2: Servidor de aplicaciones

Eso deja a JBoss AS 7 y GlassFish como las opciones posibles de selección. Debido a la integración con el IDE Netbeans utilizado para el desarrollo de la aplicación se escoge a GlassFish como servidor de aplicaciones.

5.4.2.2 Servidor de Aplicaciones GlassFish

El controlador del MVC utilizado corresponde al servidor de aplicaciones de código abierto GlassFish. Este servidor implementa las características definidas en la plataforma Java EE y permite ejecutar aplicaciones que siguen esta especificación. Es gratuito, de código libre y se distribuye bajo un licenciamiento dual a través de la licencia CDDL (Licencia Común de Desarrollo y Distribución) y la GNU GPL. Está diseñado para la implementación de Java Servlets y Java Server Pages, brindando un ambiente para programar en Java y un servidor web HTTP Java. Ideal para

aplicaciones web hechas en JAVA de gran complejidad que necesitan escalabilidad y alta disponibilidad.

Administración de GlassFish

La consola de administración permite la configuración de seguridad, despliegue de aplicaciones, cambio de contraseña, iniciar, detener o reiniciar el servicio, etc. Para ingresar en la consola se debe escribir la URL http://localhost:4848 en un navegador web. El nombre de usuario y contraseña es, por defecto, ***admin / adminadmin***. Adicionalmente es aconsejable hacer una copia del dominio para hacer pruebas y además se puede realizar un script para Iniciar/Detener/Reiniciar el servicio GlassFish.

5.4.3 MVC: Capa Vista

La capa Vista es la interface presentada al usuario, a través de la cual interactúa con el sistema; esta capa está conformada por páginas JSP donde se realizaran las peticiones a la capa modelo y el manejo de variables de sesión. Estas páginas se desarrollan conjuntamente con CSS y JavaScript para diseño y animación.

JSP, acrónimo de Java Server Pages, es una tecnología orientada a crear páginas web con programación en Java. Los JSPs se ven como páginas HTML, pero a diferencia de HTML, generan contenido dinámico. Los JSPs son abstracciones ya que son traducidos en programas java conocidos como servlets. El programa que los traduce en servlets es conocido como motor servlet. Los servlets contienen solamente código java. Todo el texto plano del JSP ha sido traducido en sentencias escritas de modo que puedan ser ejecutadas por el motor servlet.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Lo interesante de un JSP es que el motor servlet implementa la mayoría de los detalles automáticamente.

Localización JSP

La localización de los scripts JSP es en el directorio raíz de la aplicación web, no dentro del directorio WEB-INF, ya que este directorio no es accesible directamente a través de un navegador web.

Gestión de un JSP

Si existe un pedido hecho al servidor web para un JSP, el servidor debe enviar los datos del JSP a un programa especial conocido como motor servlet que manejará el pedido. Un motor servlet es un programa ejecutándose en el servidor que conoce la manera de ejecutar JSPs y servlets.

Controlador

La tarea del controlador es determinar la siguiente página a ser mostrada. Una aplicación web necesita ser capaz de enviar información de una página a otra. Todos los datos que están en los elementos de un formulario son enviados a cualquier página cuando el botón del formulario es presionado.

Las páginas que tienen elementos visibles para ingresar datos pueden fácilmente enviar datos a otra página. Basado en el botón que el usuario presione, el controlador direccionará la petición al JSP correcto. Un controlador puede ser escrito como un JSP, pero es mejor escribir el controlador como un java Servlet.

El controlador contiene únicamente código Java, no existe HTML dentro de él. Los JSPs son diseñados para tener HTML

combinados con código Java. Por lo que, el controlador debe ser escrito como un servlet, no como un JSP.

5.4.4 Arquitectura final

La ilustración de la arquitectura solución se encuentra en la Figura 5-2, donde se distingue las funciones de cada capa de acuerdo al diseño de la aplicación desarrollada.

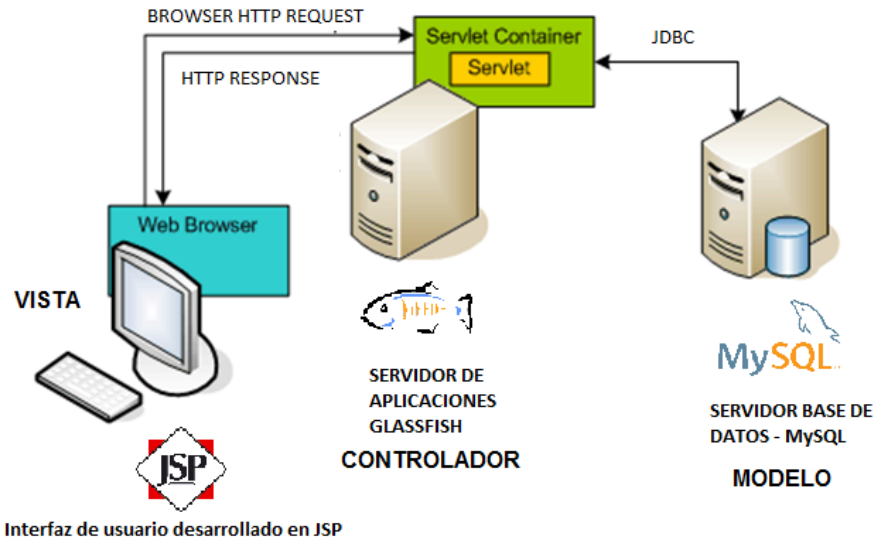


Figura 5-2: Representación MVC de Aplicación Desarrollada

5.5. Comunicación con la Central de Alarma del cliente

La comunicación con la central de alarma se obtiene mediante una aplicación java socket ejecutándose en el servidor. Esta es una aplicación cliente – servidor, ya que la aplicación se encuentra escuchando un puerto determinado a la espera de que se realice una solicitud de conexión por parte del cliente a través de la central de alarma instalada en el domicilio del usuario. Una vez que se ha establecido conexión, el intercambio de información respecto al estado y configuración de los sensores, inicia a través del protocolo PP tal como se muestra en la Figura 5-3.

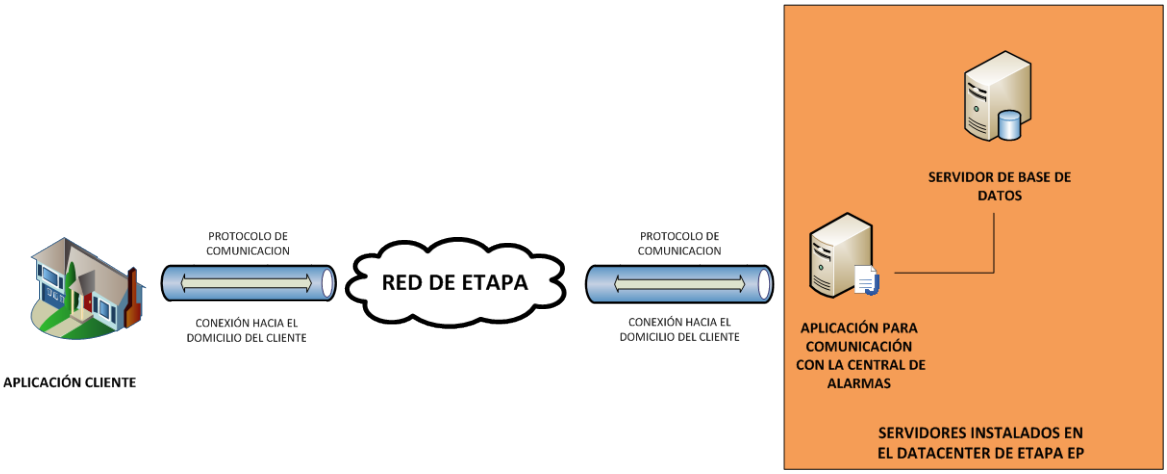


Figura 5-3: Comunicación servidor – central de alarma

CAPÍTULO 6

IMPLEMENTACION Y PRUEBAS DEL SISTEMA

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 6 IMPLEMENTACIÓN Y PRUEBAS DEL SISTEMA

6.1 CONFIGURACIÓN DEL SERVIDOR

6.1.1 Instalación del Sistema Operativo Servidor

El sistema operativo elegido es CentOS 6.4, versión de 64 bits, que es una versión estable de CentOS y puede ser actualizado a su última versión. El servidor se instaló en una PC de escritorio que cubre los requerimientos mínimos de Hardware (visto en el Capítulo 5.2.1). En la Tabla 6-1 se describen las características más importantes del equipo.

Característica	Descripción
Arquitectura	64 bits
Disco Duro	80 Gb
Lector de CD/DVD	Si
Tarjeta de audio	Si
Procesador	Intel ® Core™ 2 Duo 2.53 GHz
Memoria RAM	2 Gb

Tabla 6-1: Características de Hardware de la PC de escritorio.

Para el propósito de esta tesis se ha instalado los servidores en este ordenador. Aunque cabe recalcar que para un manejo adecuado se debería tener servidores por separado uno para Aplicaciones y otro para Base de Datos.

En cuanto a su ubicación física el servidor se encuentra en el Data Center de ETAPA EP, en un cuarto que cuenta con UPS (Uninterruptible Power Supply) por si se presenta una falla de energía.

En la configuración de red del servidor se utilizó una IP pública, mediante la cual se realizarán las pruebas del prototipo. Los parámetros utilizados en la configuración son:

- IP: 201.238.176.20
- Mascara: 255.255.255.224
- Gateway: 201.238.176.30
- DNS Primario: 191.100.0.4

6.1.2 Configuración del Servidor de Aplicaciones

Instalación y Configuración

Para instalar GlassFish en el servidor CentOS primero se debe instalar el JDK (Java Development Kit), este se lo puede descargar de la página de Oracle en su versión de 64 bits.

Se puede descargar la última versión de GlassFish en la página *http://glassfish.java.net/*, para la instalación se pueden basar en el tutorial de instalación [53].

Una vez instalado se debe configurar GlassFish desde navegador web, para ello se ingresa a la dirección http://localhost:4848 con la contraseña por defecto de GlassFish (***admin / adminadmin***). Por motivos de seguridad se debe cambiar esta contraseña.

Creación y configuración del Certificado Digital

Para crear una comunicación segura por medio del protocolo HTTPS se crea un certificado digital autofirmado utilizando la herramienta *keytool* de java, la cual tiene como función asegurar la identidad del servidor y proporcionar las claves de cifrado.

Para generar el certificado autofirmado se debe generar un par de claves (pública/privada) que se guardan en el certificado, con

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

esto se crea un almacén de claves (*keystore*) donde se guardará el certificado autofirmado con el par de claves.

Debido a que se utiliza un certificado autogenerado para aplicar SSL (Secure Socket Layer) al servidor de aplicaciones, se le debe asignar el nombre, el nombre de la unidad organizativa, el nombre de la organización, el nombre de la ciudad, el nombre de la provincia y el código postal del país.

Para generar el certificado se ejecuta el *keytool* desde el directorio donde se crea el keystore y el certificado. Para la validez del certificado generado en *keystore.jsk* dentro del archivo ***server.cer*** se debería mandar el fichero "***server.cer***" a una entidad certificadora reconocida, por ejemplo VeriSign, para que devuelva el certificado firmado. En este caso como se trabaja a nivel de prototipo se autofirmará el certificado. Como el certificado no está reconocido por el *keystore*, ni por el *cacerts keystore*, se lo debe instalar. El *cacerts keystore* es el almacén de certificados que viene por defecto cuando se instala JDK o JRE

Configuración del Certificado Digital en GlassFish

Una vez que se generaron el *keystore.jsk* y el *cacerts.jsk* hay que configurarlos en GlassFish, para ello se ingresa en la consola de GlassFish, en la opción ***server-config / SSL.*** Se habilita SSL3 y TLS y además se debe indicar la dirección donde se encuentran el keystore.jsk y el *cacerts*.jsk, como se muestra en Figura 6-1.

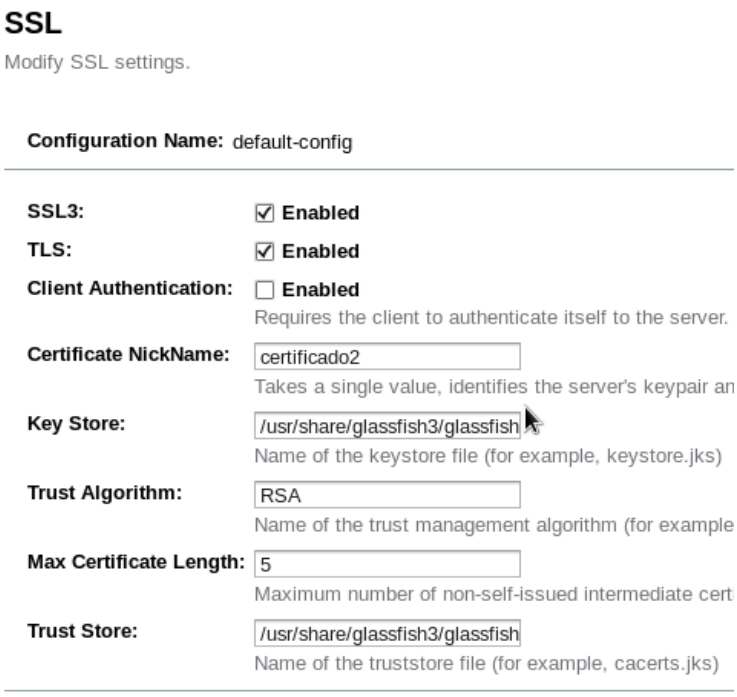


Figura 6-1: Configuración del certificado digital en la consola de GlassFish

Para probar que el certificado digital está correctamente instalado, se debe ingresar al navegador y cargar una aplicación web digitando *https://localhost:8080/AiA*. Para ver la información del certificado se ingresa en ***View Certificate***, que contiene la información del certificado, como se muestra en Figura 6-2.

Figura 6-2: Información del certificado digital en el navegador.

6.1.3 Administración del Servidor Base de Datos

Se utiliza MySQL Workbench, para poder administrar, crear y dar mantenimiento a la base de datos MySQL mediante una interface visual. Una vez instalado se debe ingresar en MySQL Workbench y crear una conexión con la base de datos MySQL.

6.1.4 Configuración de *TigerVNC* para manejo de escritorio remoto

Para poder acceder y administrar al servidor remotamente se utiliza el software *TigerVNC*. Para acceder al escritorio remoto se necesita configurar una contraseña y el número del administrador en archivo de configuración. El administrador ingresa al escritorio mediante la dirección IP del servidor seguido del número previamente configurado. Para acceder desde una terminal Linux o Windows se ingresa desde la aplicación *TigerVNC Viewer* que viene por defecto en el sistema operativo CentOS y se puede descargar desde Internet.

6.1.6 Instalación y configuración del demonio Cron

Cron es un demonio propio del sistema operativo Linux que permite ejecutar procesos o tareas que son repetitivas cada cierto tiempo. Mediante este demonio se puede ejecutar cualquier script a una hora predeterminada, según se especifique en el archivo *crontab*. El archivo *crontab* guarda el comando o script a ejecutar en la hora determinada. Se utiliza este demonio para ejecutar el script TimeLapse.sh una vez al día.

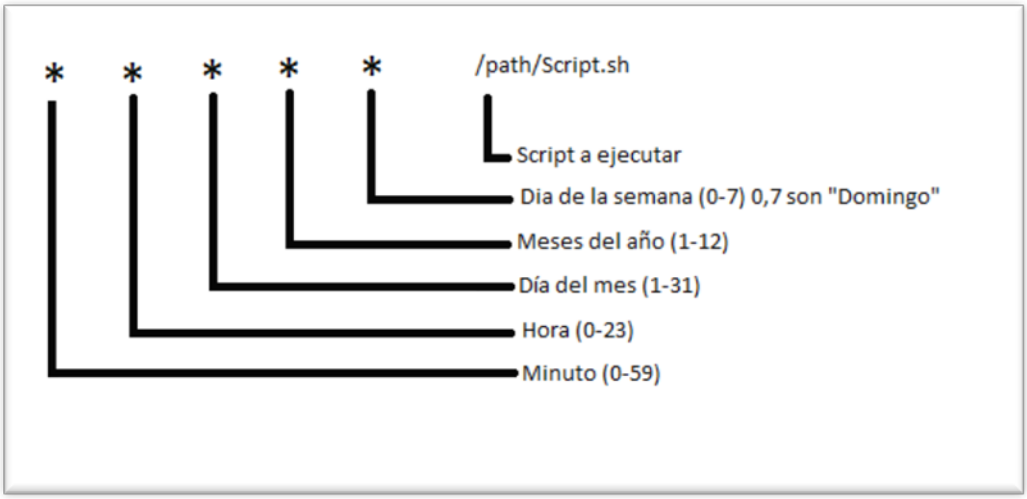


Figura 6-3: Parámetros utilizados por Crontab

En la figura 6-3, se observa los parámetros que se pueden cambiar al programar un trabajo y el significado de cada uno. Por ejemplo, para ejecutar el script TimeLapse.sh a las 3 horas con 5 minutos:

```
5  3  *  *  * /usr/sbin/TimeLapse
```

6.1.7 Creación y configuración del script TimeLapse.sh

Time-Lapse es la creación de video a partir de imágenes tomadas cada cierto intervalo de tiempo, para hacerlo se puede utilizar la aplicación *mencoder* y se necesita tener instalado los paquetes de *ffmpeg.* Este programa permite crear el video con todas las fotos que se han capturado por la cámara IP.

Descripción del funcionamiento del script

Cuando se ejecuta el script se busca las imágenes dentro de la carpeta del usuario, en caso de encontrarlas creará una carpeta que lleva como nombre la fecha-hora del sistema, por ejemplo “14.06.21_22.45”. Dentro de esta carpeta crea otra con el mismo nombre. Las imágenes capturadas por la cámara IP son cortadas y pegadas en esta carpeta y además se crea un archivo de video con extensión *.avi*.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Una vez creado el script se le da los permisos necesarios y se hace que se ejecute desde cualquier ruta que se encuentre, para ello se lo debe copiar en la carpeta sbin.

6.2 CONFIGURACIÓN APLICACIÓN SERVIDOR

6.2.1 Programación JSP y Servlet

El desarrollo de la aplicación web del sistema está basado en páginas JSP, JavaScript y CSS para estilo y animación. Todas estas herramientas de programación web conforman la interface con la que interactúa el usuario.

El IDE utilizado para el desarrollo de la aplicación web es NetBeans. Este es un entorno de desarrollo libre, hecho principalmente en lenguaje Java. Existe además un número importante de módulos para extender sus funcionalidades. NetBeans IDE es un producto libre y gratuito sin restricciones de uso.

6.2.2 Aplicación Web

El código de la aplicación web del proyecto se encuentra ubicado en dos carpetas principales: **WEB INF** y **Source Packages**. Dentro de la carpeta WEB INF se encuentran las diferentes carpetas que forman parte de la aplicación web.

Las carpetas y archivos contenidos dentro de **WEB INF** son:

- ***Carpeta CSS:*** contiene las hojas de estilo de la aplicación
- ***Carpeta Images:*** contiene las imágenes utilizadas por la aplicación Web
- ***Carpeta Js:*** contiene los archivos JavaScript que utilizan las páginas web del sistema.
- ***Páginas JSP:*** despliegan la interface web de la aplicación de los usuarios.

- ***Package aia:*** Contiene las clases java que forman parte de la aplicación: beans y el controlador servlet.

6.2.2.1 Interfaz de la aplicación web

La interfaz de la aplicación web está conformada por páginas JSP que permiten el ingreso al sistema, gestión de alarmas, gestión de usuarios y video vigilancia de acuerdo a las funcionalidades diseñadas para cada usuario del sistema tal como se muestra en el Anexo A (Funciones usuario – aplicación).

Las interfaces para cada usuario se encuentran dentro de las siguientes páginas JSP:

1. **Index.jsp.-** Esta página es la que permite el ingreso al sistema (Figura 6-4). Trabaja conjuntamente con MySQL para la autentificación de usuarios y con hojas de estilo para la presentación de las páginas web.

Figura 6-4: Página de ingreso al sistema

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

2. **Administrador.jsp**.- Esta página se muestra en la Figura 6-5 y provee al usuario autentificado como administrador las siguientes funcionalidades:

    - Gestión de usuarios: permite agregar, actualizar y eliminar usuarios.
    - Crear y configurar un sistema de seguridad para los usuarios registrados en el sistema.
    - Cambiar clave y usuario de acceso tanto personal como para los usuarios del sistema.
    - Actualización de datos personales

Figura 6-5: Página de inicio del usuario Administrador

3. **Monitoreo.jsp**.- Esta página se muestra en la Figura 6-6, está provee al usuario encargado del monitoreo del sistema de seguridad las siguientes funcionalidades:

    - Tener conocimiento del estado de los sensores instalados en el domicilio.
    - Visualización de video en vivo de las cámaras configuradas en el hogar de los clientes

- Acceder a información del usuario que permita su inmediata localización en caso de que se produzca un evento.
- Cambiar la clave de acceso personal al sistema
- Actualizar datos personales

Figura 6-6: Página de inicio del usuario monitoreo

4. **Usuario.jsp**.- Esta página se muestra en la Figura 6-7 y provee al usuario final las siguientes funcionalidades:
    - Activar y desactivar el sistema de alarmas.
    - Clasificar los diferentes sensores en tres diferentes zonas
    - Activar y desactivar el sistema por zonas
    - Cambiar clave y usuario de acceso personal al sistema
    - Visualización del video capturado por las cámaras de seguridad instaladas.
    - Acceso a carpeta FTP personal, para visualización de imágenes capturadas por las cámaras en caso de que se produzca algún evento.

- Activación del botón de pánico en caso de que se requiera auxilio inmediato

Figura 6-7: Página de inicio del usuario Cliente

6.2.2.2 Acceso a la base de datos

Para la conexión entre la aplicación web y la base de datos, se utiliza el driver JDBC para MySQL conocido como Connector/J. El Connector/J es diseñado específicamente para MySQL e intenta adherirse al API JDBC tanto como sea posible.

Establecimiento de conexión

Para establecer la conexión con la base de datos se debe tener el servidor MySQL iniciado. El servidor MySQL abre por defecto el puerto 3306 para aceptar conexiones de posibles clientes, y de programas que requieran conectarse y acceder a la base de datos. La aplicación web desarrollada, al requerir consultar las tablas contenidas en la base de datos, deberá conectarse a este servidor.

Para establecer la conexión desde java, la clase DriverManager tiene el método getConnection(). Este método se utiliza de la siguiente manera:

```
Connection conexion = DriverManager.getConnection
("jdbc:mysql://localhost/mydbsecurity","root", "password");
```

El primer parámetro del método **getConnection()** es un **String** que contiene la *url* de la base de datos:

- **jdb:mysql:** debido a que se está utilizando un driver JDBC para MySQL.
- **localhost**: debido a que el servidor de base de datos se encuentra en el mismo ordenador. Aquí puede colocarse una IP o un nombre de máquina que esté en la red.
- **mydbsecurity:** es el nombre de la base de datos a la que se desea conectar

Los otros dos parámetros son dos String que corresponden al nombre de usuario y password para acceder a la base de datos. Al instalar MySQL se crea el usuario root y se pide el password para él.

Si todo está correcto, se establecerá una conexión exitosa a la base de datos. Esta conexión es en realidad un socket entre java y la base de datos, aunque para el usuario es transparente.

6.3 Configuración del sistema mediante la Aplicación Web

Con el fin de verificar el correcto funcionamiento y comunicación entre la aplicación desarrollada y la central de alarma, se procede a la creación de un cliente al que se le configurará un sistema de alarmas para su posterior monitoreo.

Creación del cliente

1. Se ingresa a la aplicación a través del explorador digitando la siguiente dirección: http://201.238.176.20:8080/AiA/ .

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

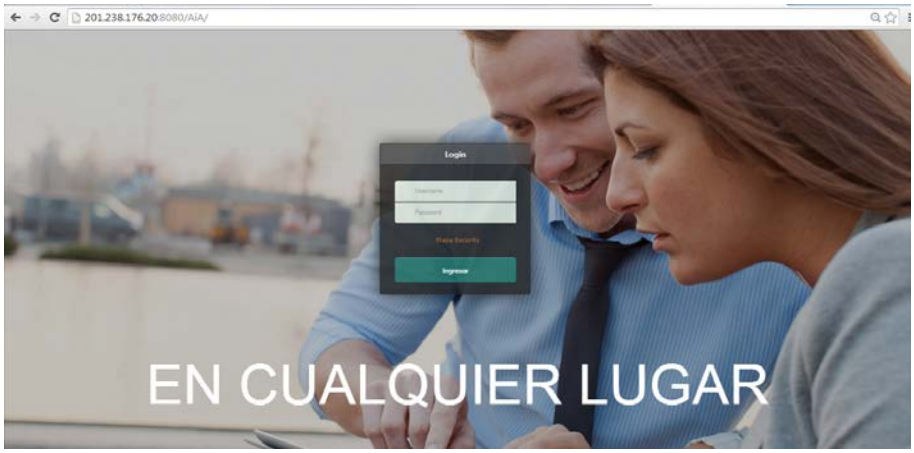


Figura 6-8: Página de inicio de la aplicación

2. La primera página desplegada por defecto es la página de autentificación. En ella se pide que se ingrese los datos de usuario y contraseña, necesarios para ingresar al sistema. Una vez realizada la autentificación, (Figura 6-8), se presentará la página que contiene las funcionalidades diseñadas para el usuario “administrador” (Figura 6-9)

Figura 6-9: Funcionalidades usuario “Administrador”

3. Dando clic sobre la opción “CLIENTES” se desplegará la página que contiene las funcionalidades diseñadas para la

gestión de los usuarios que conforman el sistema como se muestra en la Figura 6-10.

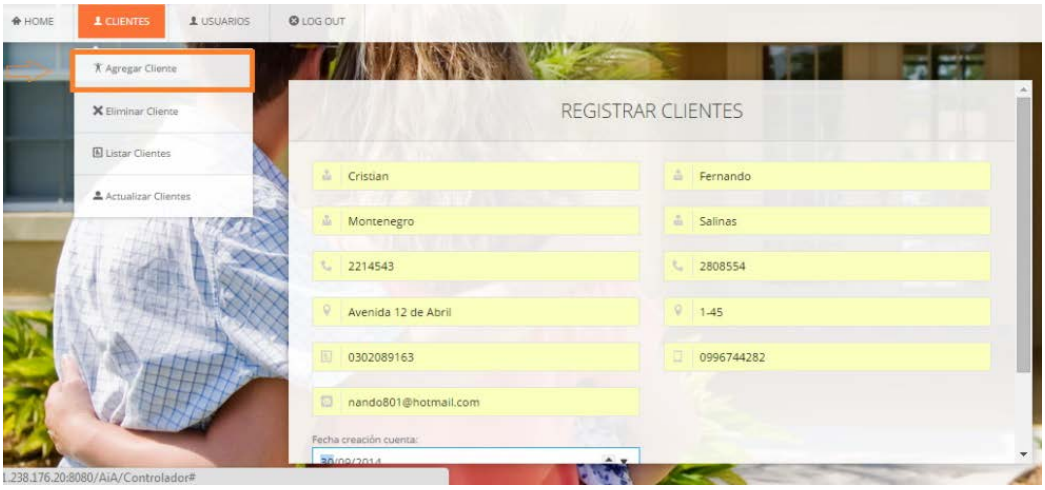


Figura 6-10: Página encargada de la gestión de usuarios del sistema.

4. Dando clic sobre la pestaña CLIENTES (Figura 6-10) se desplegaran las opciones disponibles, entre las que se encuentran:
    - Agregar Cliente
    - Eliminar Cliente
    - Listar Cliente
    - Actualizar Datos
5. Se escoge la opción “Agregar Cliente”, la misma que desplegará un formulario para registrar al cliente. Una vez completados todos los campos, se procede a presionar el botón “Agregar” como se muestra en la Figura 6-11.

Figura 6-11: Formulario para ingreso de clientes al sistema

6. Con el fin de comprobar que el cliente ha sido ingresado exitosamente, se procede a listar los usuarios ingresados tal como se muestra en la Figura 6-12.

Figura 6-12: Formulario para ingreso de clientes al sistema

7. Una vez registrado el cliente, se retorna al menú principal dando clic sobre la pestaña “HOME” (Figura 6-13)

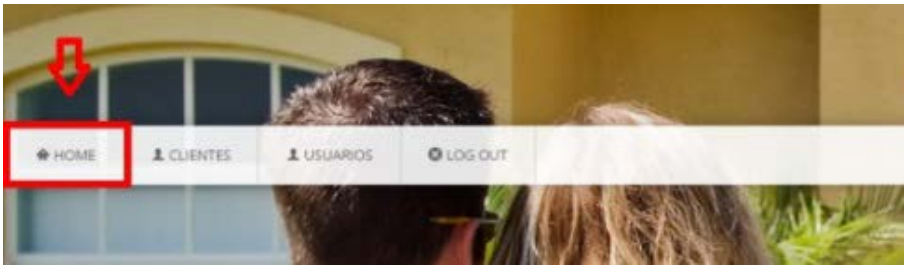


Figura 6-13: Formulario para ingreso de clientes al sistema

Configuración sistema de alarmas

1. Luego, en el menú principal se presiona la opción “Sistema de Alarmas” como se muestra en la Figura 6-14.

Figura 6-14: Menú principal usuario “Administrador”

2. Dando clic sobre la opción “Sistema de Alarmas” se desplegará la página que contiene las funcionalidades diseñadas para la creación, configuración y consulta del sistema de alarmas del cliente (Figura 6-15).

Figura 6-15: Menú sistema de alarmas

3. Se escoge la opción “Crear Sistema”, la misma desplegará un formulario que permite elegir el usuario al que se creará el sistema (Figura 6-16) y seleccionar los dispositivos y el

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

número de dispositivos que conforman el sistema de alarmas del cliente como se muestra en la Figura 6-17.

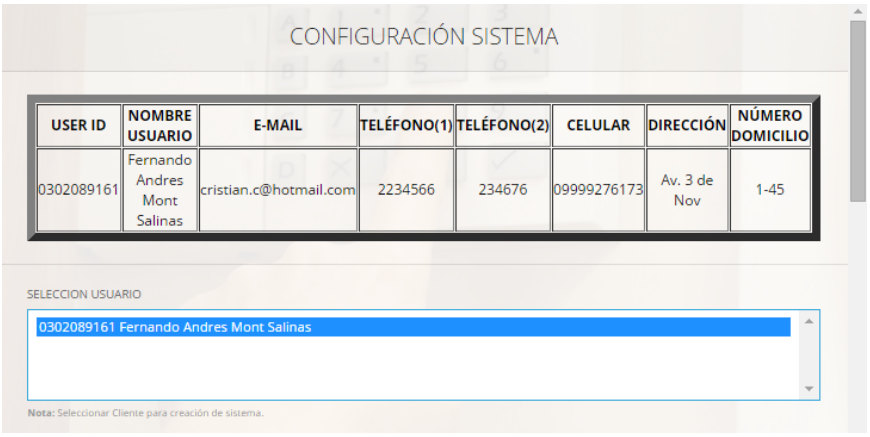


Figura 6-16: Selección de cliente.

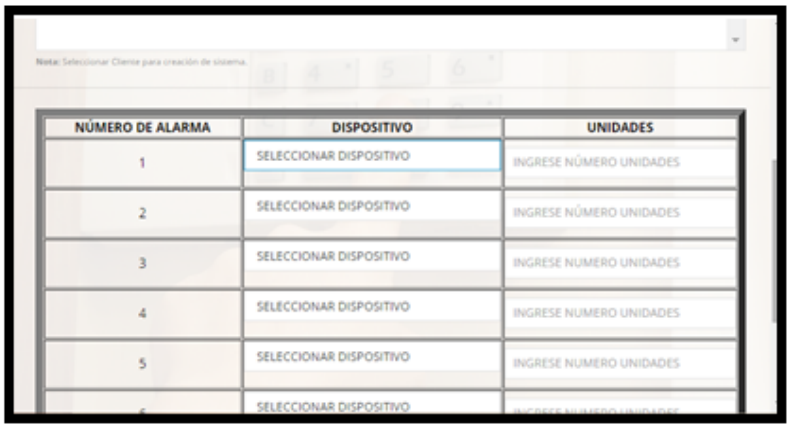


Figura 6-17: Creación sistema de alarmas

4. Luego de realizar el ingreso de los dispositivos, se procede a configurar el sistema de acuerdo a la distribución de sensores permitida. Esto se realiza al escoger la opción “Configurar Sistema” (Figura 6-18) y seleccionar el cliente al que se le configurará el sistema. Una vez finalizada la configuración, se presiona el botón “Crear Sistema” (Figura 6-19).

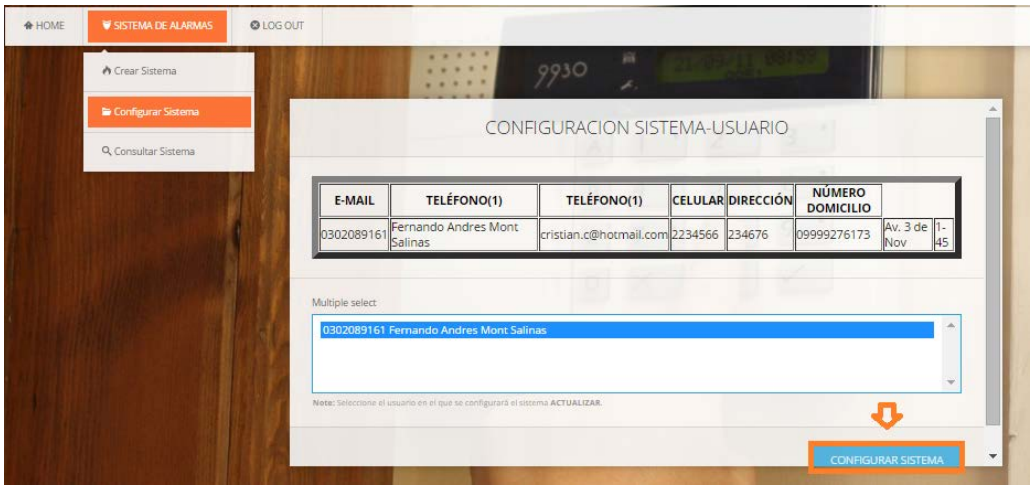


Figura 6-18: Configuración del sistema

5. En la página de configuración del sistema, se seleccionan los dispositivos que forman parte del sistema de acuerdo a las 7 distribuciones permitidas. A cada una de las distribuciones se les asigna un alias que permite identificar a cada distribución dentro del sistema Figura 6-19.

Figura 6-19: Configuración distribuciones

6. Una vez ingresado el sistema se procede a ejecutar la aplicación servidor socket, encargada de comunicarse con la central de alarmas de los clientes configurados en el sistema como se muestra en la Figura 6-20.

```
run:
Servidor a la espera de conexiones.
```

Figura 6-20: Configuración del sistema

7. Al ingresar al sistema como usuario “Cliente” se selecciona la opción “ESTADO ALARMAS” (Figura 6-21), la misma que despliega una tabla que permite visualizar el estado actual de los sensores configurados dentro de la columna llamada “ESTADO”. Inicialmente los sensores se encuentran con el Estado: “SIN GESTION”, debido a que la comunicación entre la central de alarmas y la aplicación servidor socket aún no ha sido establecida como se observa en la Figura 6-22. El estado “SIN GESTION” se representa con el color naranja.

Figura 6-21: Configuración del sistema

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Figura 6-22: Estado actual sensores

6.4 IMPLEMENTACIÓN DE LA APLICACIÓN CLIENTE

6.4.1 Selección de equipos

La descripción de las funciones y características de cada uno de los equipos seleccionados se muestran en el Anexo G, resaltando que el transformador, batería, sensor de movimiento, sensor magnético y sirena se eligieron con la idea de reutilizar los equipos existentes en los domicilios.

6.4.2 Elaboración de PCB (Printed Circuit Board) de cada modulo

El diseño de cada circuito se realizó con *KiCad*, software cuya función es la creación de diagramas y circuitos profesionales. KiCad cumple con los requerimientos para el diseño del sistema con un valor agregado que es libre y de código abierto ideal para estudiantes y desarrolladores.

Una vez diseñados los diagramas electrónicos de cada módulo y definido los equipos a utilizar se proceden a elaborar las PCBs. El método utilizado se llama popularmente método de la plancha. Primero se requiere de los impresos de cada circuito a blanco y negro sobre papel fotográfico. En las Figuras 6-23, 6-24, 6-25, 6-

26, 6-27 y 6-28 se muestran los circuitos de cada módulo previos a imprimir.

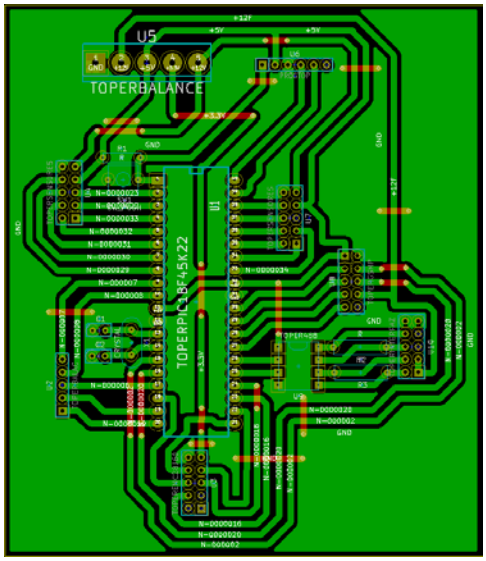


Figura 6-23: Diseño PCB del Módulo Central.

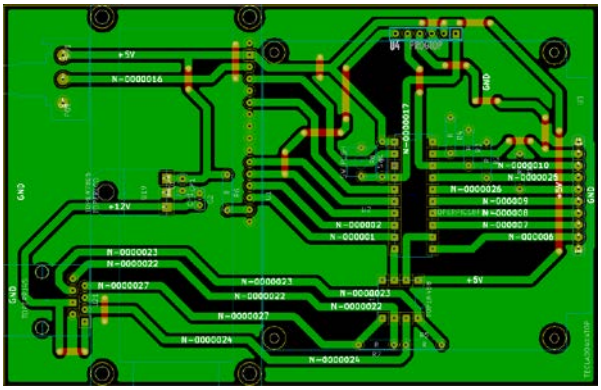


Figura 6-24: Diseño PCB del Terminal.

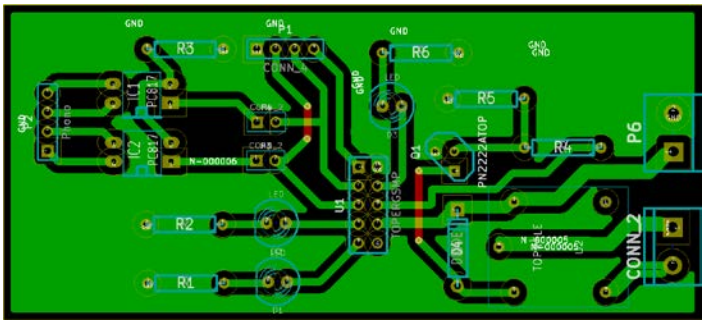


Figura 6-25: Diseño PCB del Módulo GSM-Sonido.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

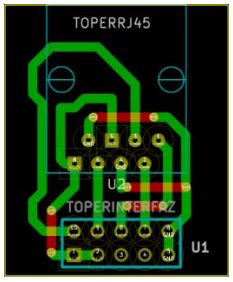


Figura 6-26: Diseño PCB del convertidor IDC-RJ45.

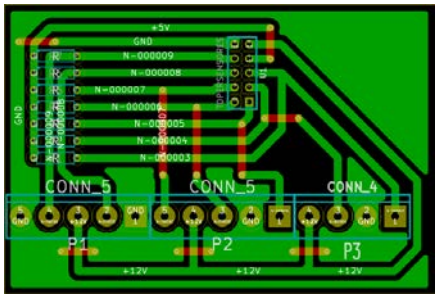


Figura 6-27: Diseño PCB del módulo sensores.

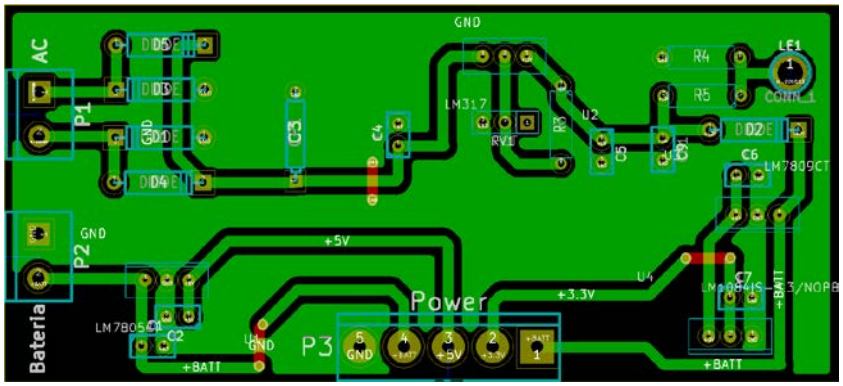


Figura 6-28: Diseño PCB del módulo Gestión de Energía.

Los circuitos impresos se colocan sobre una placa de cobre (baquelita) y se procede a pasar sobre el papel la plancha por aproximadamente 5 minutos. Cuanto la tinta se ha trasferido del papel al cobre, se procede a quitar el cobre con la ayuda de agua caliente y percloruro de hierro en un recipiente de plástico. Una vez que se tiene la placa con el circuito se realizan agujeros con un taladro según el esquema. Finalmente se colocan los elementos y

se los suelda. Como resultado se tiene las placas ya terminadas y se muestran en las Figuras 6-29, 6-30, 6-31, 6-32, 6-33 y 6-34.

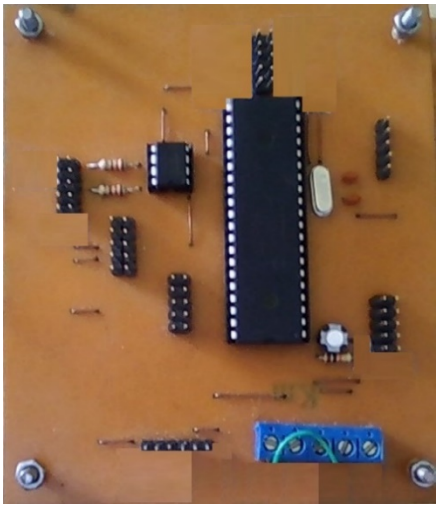


Figura 6-29: Fotografía del módulo Central

Figura 6-30: Fotografía del Terminal

Figura 6-31: Fotografía del Módulo GSM-Sonido

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

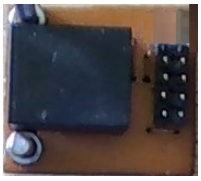


Figura 6-32: Fotografía del convertidor IDC-RJ45.

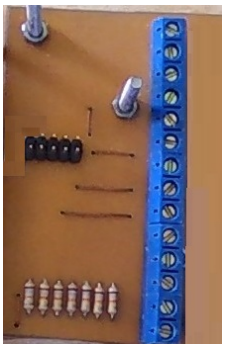


Figura 6-33: Fotografía del Módulo Sensores.

Figura 6-34: Fotografía del Módulo Gestión de energía.

6.4.3 Programación de la Central de Alarma

Con MikroC PRO for PIC para la programación, se implementa las funcionalidades del módulo central y del panel de usuario, en los microcontroladores PIC18F45K22 y PIC18F14K22 respectivamente.

Programación del panel de usuario: Se inicia con la configuración del PIC mostrada en la Figura 6-35, donde se define el PIC a utilizar, la frecuencia del oscilador, etc. En este caso se

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

dejan las configuraciones por defecto y se las realiza vía línea de comandos.

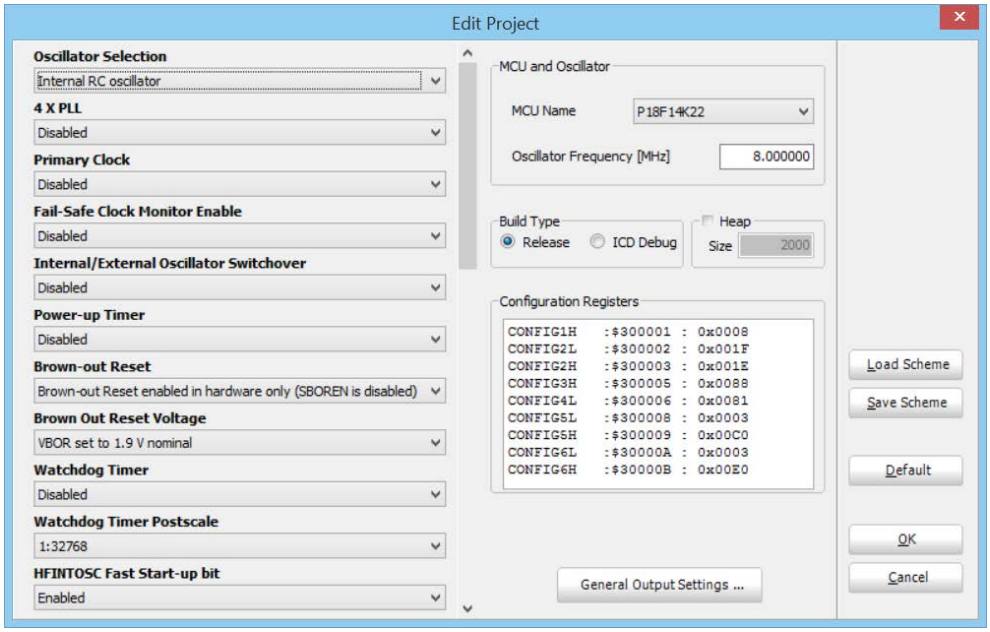


Figura 6-35: Configuración inicial en MikroC del PIC18F14K22.

El código del programa cuenta con una función principal llamada *main()* y funciones secundarias que son llamadas desde *main()*. A continuación se describen las funciones secundarias:

- **ClicBoton():** Permite ingresar datos del usuario a través del teclado.
- **Enviar_PP():** Envía un paquete de datos PP.
- **CargarDatos():** Carga los datos en el paquete PP.
- **Recibir_PP():** Recibe paquetes PP.
- **Interrupt():** Función por defecto en MikroC para ejecutar código en caso de generarse una interrupción.
- **main():** Función principal del programa, aquí se realizan las configuraciones iniciales, se definen variables y llama funciones.

Programación del módulo central: La configuración se realiza de igual manera que el terminal, excepto por el nombre del MCU. Las funciones secundarias utilizadas son:

Funciones secundarias:

- **LlamarGSM():** Realiza una llamada para advertir la detección de un evento.
- **Enviar_PP():** Envía un paquete de datos PP.
- **CargarDatos()**
- **Recibir_PP()**
- **Interrupt()**
- **ComunicaciónNormal():** Esta función se ejecuta cuando todo está bien, es decir no hay problemas de energía y hay conexión con el servidor. Entonces Intercambia datos con la "aplicación servidor" para actualizar el estado de los sensores.
- **ComunicaciónBasica():** Esta función se ejecuta cuando hay problemas de energía o no hay conexión con el servidor. Entonces la única manera de comunicarse con el servidor es a través de GSM. Además esta función no permite configurar sensores mientras no se establezca comunicación con la aplicación servidor.
- **Configuración():** Aquí se realizan la configuración iniciales del PIC.

A más de las funciones antes definidas, se dispuso de librerías propias de MikroC para agilitar el desarrollo del programa.

A continuación se describen las funciones más importantes de la librería Net_Ethernet_28j60.

- **Net_Ethernet_28j60_Init:** Rutina indispensable para el funcionamiento correcto de todas las librerías, ya que se establecen parámetro principales de funcionamiento.
- **Net_Ethernet_28j60_stackInitTCP:** Rutina requerida para inicializar el stack TCP.
- **Net_Ethernet_28j60_confNetwork:** Rutina donde se establecen parámetros adicionales, por ejemplo: la dirección IP del Gateway.
- **Net_Ethernet_28j60_UserTCP:** Rutina donde se implementa la aplicación deseada, en este caso SOCKET.
- **Net_Ethernet_28j60_disconnectTCP:** Rutina encargada de finalizar la conexión TCP establecida.
- **Net_Ethernet_28j60_putByteTCP:** Rutina cuya finalidad es tomar los datos del usuario a ser enviados y colocarlos en el búfer Tx.
- **Net_Ethernet_28j60_connectTCP:** Rutina para establecimiento de conexión.
- **Net_Ethernet_28j60_startSendTCP:** Rutina que alista los parámetros y datos TCP para empezar el envío.
- **Net_Ethernet_28j60_doPacket:** Rutina que se debe llamar en toda aplicación y con la mayor frecuencia posible ya que es la encargado de llamar a rutinas para gestión de paquetes.
- **Net_Ethernet_28j60_getByte:** Rutina para leer los bytes recibidos.

6.4.4 Configuración de Video

Una vez realizada la configuración de la cámara IP (ver Anexo C) en la LAN del usuario, se ingresa a la aplicación como usuario-cliente. Para realizar el registro de la cámara se debe hacer clic en la pestaña *configurar cámara* (Figura 6-36).

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

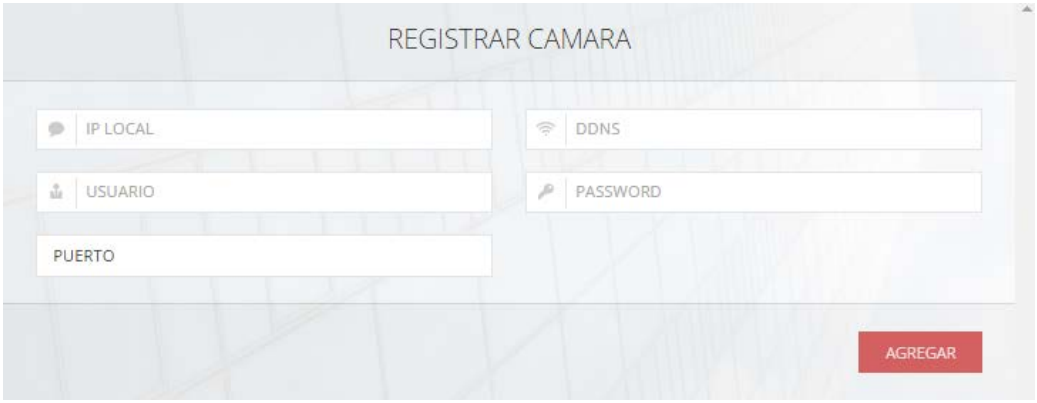


Figura 6-36: Ventana para la configuración de la cámara de un usuario

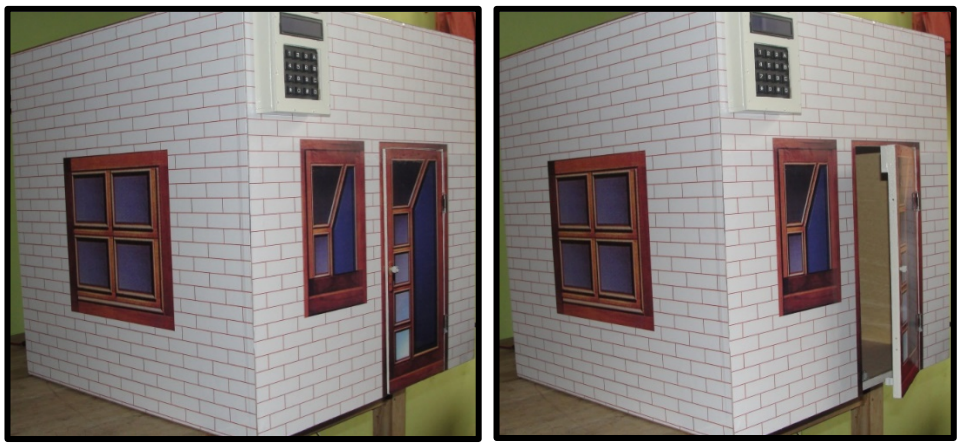
Se ingresa la IP privada del cliente, la dirección para manejo de IP Dinámica, DDNS (ver Anexo D), el usuario y contraseña del administrador de la cámara y el puerto que va a utilizar para comunicarse.

Para verificar que la configuración se realizó de manera correcta se ingresa en la pestaña listar cámaras y se observa las direcciones privada con la cual ingresa el usuario desde su LAN y la dirección DDNS con la cual ingresa desde la red WAN.

6.4.5 Montaje de la solución

Para la implementación del sistema se construyó una maqueta que simule un domicilio. Con dimensiones de 50x50x50cm. Esta posee una puerta para la instalación del sensor magnético con el fin de detectar su apertura. En la Figura 6-37 (a) y (b) se muestra una imagen de la maqueta con la puerta cerrada y abierta respectivamente. Además también se observa la instalación del panel de usuario.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas



(a) Maqueta con la puerta cerrada (b)Maqueta con la puerta abierta

Figura 6-37: Fotografía de la maqueta que simula un domicilio

Dentro de la maqueta se instaló un gabinete donde se ubican cada uno de los módulos desarrollados. También se instaló un sensor de movimiento. En la Figura 6-38 se observa la ubicación del gabinete, sensor de movimientos y sirena.

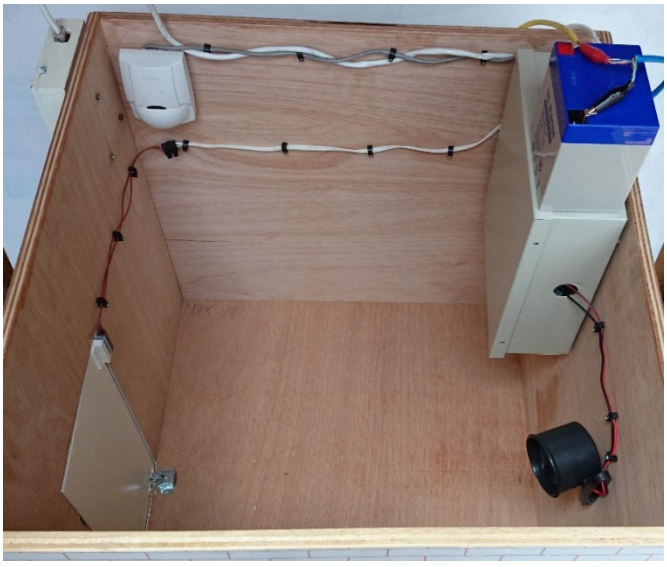


Figura 6-38: Fotografía de la ubicación del gabinete y sensor de movimiento

Para finalizar la implementación se necesita conectar la central de alarma a un modem con acceso a internet.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

6.4.6 Pruebas locales de la central de alarma

Para probar que el sistema funcione correctamente y obtener valores que permitan hallar las limitantes del sistema, como por ejemplo el consumo de energía de cada módulo, el tiempo de respaldo de energía por parte de la batería, se realizan las siguientes pruebas.

6.4.6.1 Pruebas de consumo de energía

Todas las pruebas son realizadas de manera básica y con el uso del multímetro en los elementos que se consideraron como principales, sin considerar disipación de potencia por temperatura, regulación de voltaje, resistencia del conductor, etc, con el fin de saber el consumo de corriente de cada módulo.

Panel de usuario: Tiene un consumo promedio de 67.5mA sin tener mayor variación en sus valores. La potencia seria de:

$$67.5mA * 14V = 0.945W.$$

Modulo central: Tiene un consumo promedio de 53.75mA, dando como resultado una potencia de:

$$53.75mA * 14V = 0.753W.$$

Sirena: Tiene un consumo de 750mA, dando como resultado una potencia de:

$$750mA * 14V = 10.5W.$$

Módulo GSM: Tiene un consumo de 750mA, dando como resultado una potencia de:

$$990mA * 14V = 13.86W.$$

Sensores: El consumo de corriente depende del tipo y número de sensores conectados a la central de Alarma, en general el

consumo de corriente sin conectar sensores es de 3.5mA. Los sensores magnéticos consumen corrientes en el orden de los microamperios, se los puede despreciar. Los sensores de movimiento consumen en promedio 10mA y su voltaje de operación es de 9.6 a 16V.

En el caso que se conectan varios sensores, el consumo de energía cambia, así que se realizará el cálculo con 4 sensores de movimiento. Se obtiene una corriente total de $10mA * 4 + 3.5mA = 43.5mA$. Dando como resultado una potencia de:

$$43.5mA * 14V = 0.609W.$$

Modulo Ethernet: La potencia utilizada es de:

$$14V * 94mA = 1.316W$$

Central de alarma: Se considera el consumo de corriente de todos los elementos a excepción de la sirena y el módulo GSM. Con una potencia total de:

$$0.945W + 0.753W + 0.609W + 1.316W = 3.623W\ .$$

6.4.6.2 Pruebas del respaldo de energía

Se consideran 3 elementos debido a su alto consumo de potencia, se tiene la sirena con 10.5W, módulo GSM con 13.9W y la central de alarma pero sin considerar los dos elementos anteriores con 3.6W.

Se tiene diferentes consumos de energía según las condiciones siguientes:

Condiciones de respaldo normal: Se produce con la red eléctrica del domicilio fuera de servicio, el canal de comunicaciones entre el cliente y el servidor en perfectas condiciones y la alarma en estado no Activada. El consumo de potencia para este caso se muestra en la Tabla 6-2.

Tabla de consumo de potencia			
Central de alarma	Sirena	GSM	Total
3.6W	0W	0W	3.6W

Tabla 6-2: Consumo de potencia en condiciones de respaldo normal

Condiciones de respaldo doble: Se produce con la red eléctrica del domicilio fuera de servicio, el canal de comunicaciones entre el cliente y el servidor en malas condiciones y la alarma en estado no Activada. El consumo de potencia para este caso se muestra en la Tabla 6-3.

Tabla de consumo de potencia			
Central de alarma	Sirena	GSM	Total
3.6W	0W	13.9W	17.5W

Tabla 6-3: Consumo de potencia en condiciones de respaldo doble

Condiciones de respaldo Activo: Se produce con la red eléctrica del domicilio fuera de servicio, el canal de comunicaciones entre el cliente y el servidor en perfectas condiciones y la alarma en estado Activada. El consumo de potencia para este caso se muestra en la Tabla 6-4.

Tabla de consumo de potencia			
Central de alarma	Sirena	GSM	Total
3.6W	10.5W	0W	14.1W

Tabla 6-4: Consumo de potencia en condiciones de respaldo activo

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Condiciones de respaldo Crítico: Se produce con la red eléctrica del domicilio fuera de servicio, el canal de comunicaciones entre el cliente y el servidor en malas condiciones y la alarma en estado Activada. El consumo de potencia para este caso se muestra en la Tabla 6-5.

Tabla de consumo de potencia			
Central de alarma	Sirena	GSM	Total
3.6W	10.5W	13.9W	28W

Tabla 6-5: Consumo de potencia en condiciones de respaldo crítico

En condiciones de respaldo Crítico y respaldo activo el consumo de energía es elevado, sin embargo es un evento que hay que solucionar en el menor tiempo posible así que en este caso no se analiza el tiempo de respaldo de la batería.

En condiciones de respaldo doble el consumo de energía es elevado en comparación con otras condiciones, así que estas condiciones es la que se va a tomar como referencia para las pruebas y análisis de tiempo de respaldo de la batería.

Características de la batería: 4Ah a 12V

Consumo total de corriente = $17.5W \div 14V = 1.25A$.

La batería es de 4Ah entonces:

$$4Ah \div corriente\ total = horas\ de\ respaldo$$

$$4Ah \div 1.25A = 3.2\ Horas = 3\ Horas\ y\ 12\ Minutos$$

6.4.6.3 Pruebas de Networking local

Para el análisis del tráfico se utiliza *Wireshark*, software gratuito que dispone de varias herramientas para un análisis profundo, con el fin de determinar el *Throughput* y los tiempos en la

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

comunicación. En la figura 6-39 se muestra el resultado de la captura y análisis de paquetes.

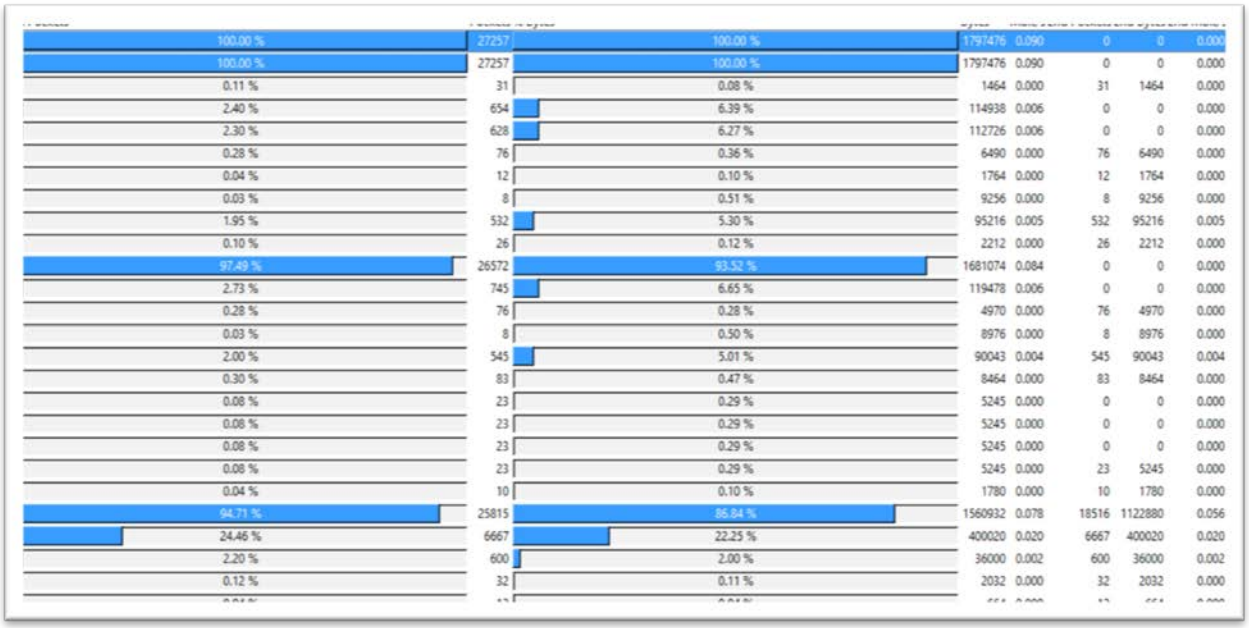


Figura 6-39: Imagen del tráfico de red con Wireshark.

Para el análisis de tráfico se consideran los siguientes datos:

Tiempo de captura: 160.122 seg

Número de Paquetes: 27257

Paquetes por segundo: 170.227

Tamaño del Paquete: 65945 Bytes

Velocidad: 90 Kbits/seg

Luego de realizar un filtrado para capturar solo paquetes TCP se obtiene lo siguiente.

25815 paquetes TCP

Velocidad: 78Kbits/seg

6667 (24.46%) paquetes inválidos

600 (2.2%) Datos

De los siguientes datos se puede decir lo siguiente:

Eficiencia: 75.54%

Throughput: 2 Kbits/seg

En la Figura 6-40 se muestra que en los primeros 25 segundos, el cliente intenta establecer conexión con el servidor pero falla e intenta otra vez hasta que a los 60 segundos, se establece la conexión. A partir de este punto hay un flujo de paquetes variable que va desde 150 a 190 paquetes por segundo.

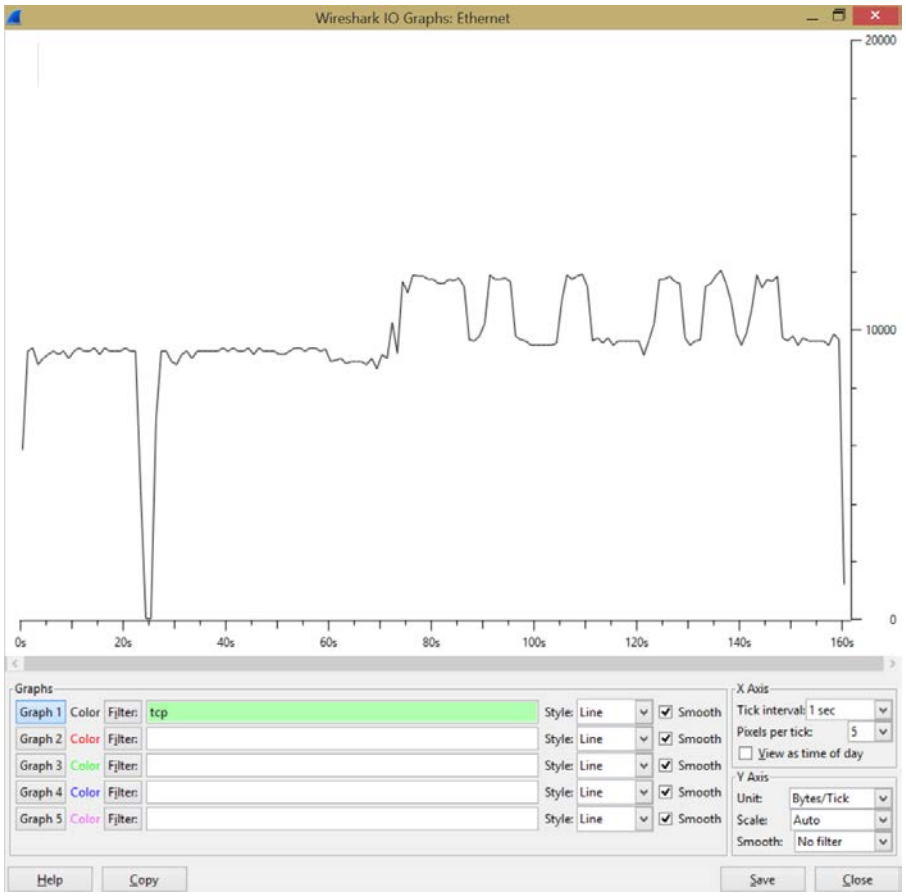


Figura 6-40: Imagen del tráfico de red con Wireshark.

La pérdida de sincronización se debe a que se maneja dos comunicaciones de manera secuencial. Los tiempos de comunicación de PP son los siguientes.

Velocidad rs232: 1308.75 Bytes por segundo.
Numero de bytes: 14 Bytes
Velocidad: 93.48 Paquetes por segundo.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

La velocidad PP y el tamaño del paquete son algunos de los factores que influyen en la sincronización del sistema. Sin embargo existen otros factores que obedecen a la configuración avanzada del módulo Ethernet y el microcontrolador.

6.4.6.4 Pruebas de distancia de conexión

Consiste en pruebas de conexión entre el terminal y el modulo central, para determinar la separación máxima entre los dos equipos, considerando los niveles de energía requeridos.

El integrado Max488 en teoría conecta dos dispositivos separados hasta una distancia de 1 Km.

La interface local consume en promedio 67.5 mA, la fuente de alimentación es de 14V, la interface local para su funcionamiento requiere un voltaje mínimo de 8 V según el integrado 7805, entonces:

$resistencia\ total\ (rt)$

$distancia\ (d)$

$resistencia\ por\ metro\ (rm)$

$$rt = d * rm$$

$$rt = d * 0.289$$

$$atenucion(a) = rt * corriente\ terminal(ct)$$

$$a = d * 0.289 * ct = d * 0.289 * 0.0675 = d * 0.0195$$

$$a = voltaje\ fuente(vf) - voltaje\ minimo(vm)$$

$$a = vf - vm = 14V - 8V = 6V$$

$$d = a \div 0.0195 = 307.69\ metros$$

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

La distancia máxima es 308 metros para que la interface local sea alimentada con un nivel de voltaje aceptable.

Como 308 metros es menor a 1000 metros, se considera los 308 metros como la distancia de separación máxima en teoría.

Las pruebas realizadas a nivel de laboratorio se efectuaron a una distancia de 25 metros sin encontrar inconvenientes en el funcionamiento.

Para determinar la distancia de separación del sensor de movimiento a la central de alarma se considera la fuente de 14 V, corriente de consumo 12 mA. Se puede determinar de manera teórica la distancia de separación máxima.

$$rt = d * 0.2890$$

$$a = rt * corriente\ sensor(cs)$$

$$a = d * 0.289 * cs$$

$$a = d * 0.0035$$

$$a = vf - vm = 14 - 9.6 = 4.4$$

$$d = a \div 0.0035 = 1257\ metros$$

Las pruebas se realizaron a 53,92m obteniendo resultados correctos en el funcionamiento.

6.5 PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA

Una vez instalado y configurado el sistema, éste se encuentra listo para su funcionamiento. Establecida la conexión, se necesita de un registro por parte del usuario mediante la central de alarma a través de un código único asignado a cada usuario para la autentificación y establecimiento de conexión con la "aplicación servidor". La "aplicación servidor" siempre está escuchando peticiones de conexión de la central de alarmas, además realizada la conexión, la central de

alarma siempre informa a la “aplicación servidor” sobre los cambios de estado en los sensores y las configuraciones hechas dentro de la interface local, y viceversa.

En la central de alarma se encuentra configurado un socket cliente, que al ser conectado a la red TCP-IP envía peticiones de conexión a la aplicación socket desarrollada en la “aplicación servidor”. La configuración del cliente socket para establecer la conexión hacia el servidor es de la siguiente manera:

IP Local: 192.168.20.61
IP Remoto: 201.238.176.20
Puerto Origen: 3333
Puerto Destino: 4444

6.5.1 Procedimiento

Configuración sistema de alarmas

1. La aplicación socket servidor se encuentra escuchando peticiones de conexión. Una vez autentificado el cliente, el servidor establecerá conexión, como se muestra en la Figura 6-41.

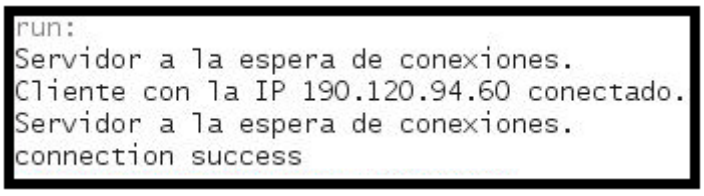


Figura 6-41: Establecimiento de conexión Central de alarmas – Aplicación servidor

2. Mediante el protocolo establecido, la “aplicación servidor” y la central de alarma comparten información respecto al estado de los sensores, configuración de zonas, activación y desactivación de alarmas según las acciones que sean ejecutadas.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

3. La aplicación permite la configuración de tres zonas de monitoreo. Cada zona puede tener sensores configurados en ella para su posterior monitoreo. Para configurar una zona, se elige la opción “CONFIGURAR ZONAS”, la que desplegará la lista de sensores y permitirá la configuración de cada sensor en una zona respectiva como se observa en la Figura 6-42.

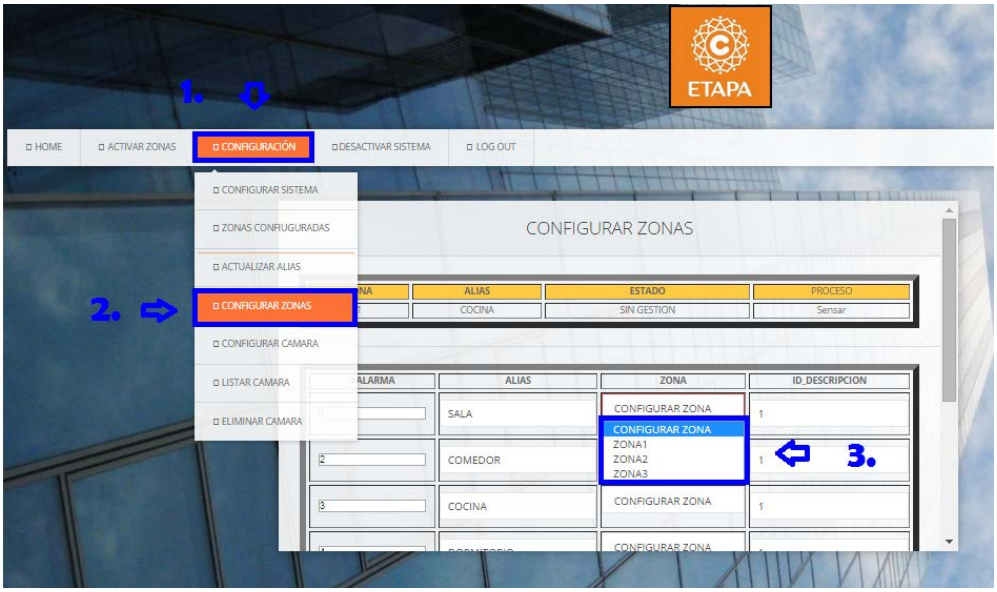


Figura 6-42: Configuración zonas

4. Una vez configurada la zona, se presiona el botón “ACTUALIZAR” (Figura 6-43)

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Figura *6-43*: Actualizar configuración zonas

5. Se verifica si la configuración se realizó con éxito, dirigiéndose a la opción “ZONAS CONFIGURADAS”, la que desplegará la lista de sensores que se encuentran configurados en determinada zona (Figura 6-44).

Figura 6-44: Zonas configuradas

6. Configurada la zona de monitoreo, se procede a activarla para que pueda ser monitoreada, tal como se muestra en la Figura 6-45.

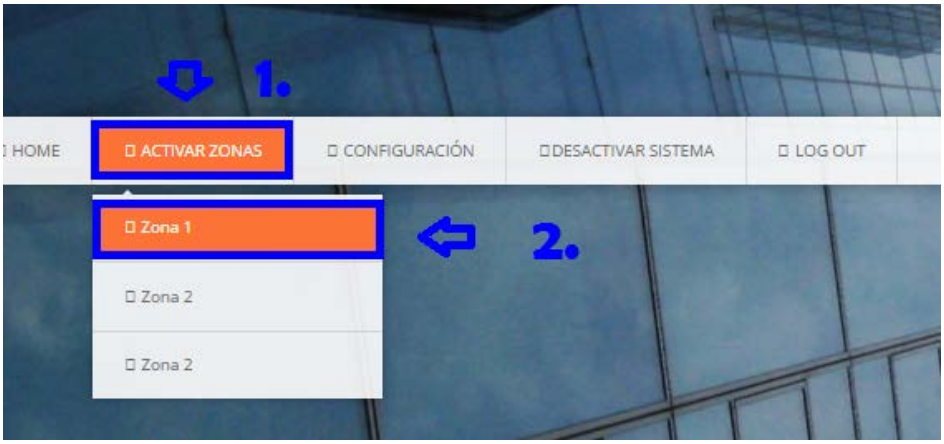


Figura 6-45: Activación zonas

7. Activada la zona, los sensores configurados en ésta son monitoreados por el sistema. El estado actual de los sensores puede ser visto desde la interface web del cliente y monitoreo ingresando a la opción “ESTADO DE ALARMAS” y

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

"MONITOREO" de cada usuario, como se muestra en las Figuras 6-46 y Figura 6-47.

Figura 6-46: Opción "ESTADO ALARMAS" interface web cliente

Figura 6-47: Opción "MONITOREO" interface usuario monitoreo

8. Al ingresar a las opciones mencionadas anteriormente, se desplegarán las páginas mostradas en las Figuras 6-48 y 6-49, las mismas contienen el estado actual de los sensores configurados en el sistema. El estado de los sensores se muestra en la columna ESTADO, al establecer conexión el estado de los sensores cambia a "NO ALARMADO" representado por color verde. Estas páginas refrescan el estado de los sensores cada cinco segundos con el objetivo de mantener actualizado el estado de los sensores. El usuario

monitoreo visualiza el estado de todos los sensores de los usuarios ingresados en el sistema.

Figura 6-48: Estado alarmas interface cliente

Figura 6-49: Estado alarmas interface monitoreo

9. Para la comprobación del funcionamiento del sistema se procede a la generación de un evento de modo que se active el sensor de la zona anteriormente configurada. El sensor configurado es el sensor número 3 ya que este se encuentra configurado en la zona activada número 1.

10. El evento generado se reflejará tanto en la interface cliente como en la de monitoreo. En las Figuras 6-50 y 6-51 se observa la alarma generada por el sensor número 3. La generación de la alarma ocasiona un cambio en la columna

ESTADO a “ALARMA ACTIVADA” representado por el color rojo.

Figura 6-50: Representación evento generado interface web cliente

Figura 6-51: Representación evento generado interface web monitoreo

11. Para normalizar el sistema, se procede a la desactivación de la alarma generada presionando el botón “DESACTIVAR SISTEMA” (Figura 6-52) ubicada dentro de la opción “ESTADO ALARMAS” de la interface web del usuario cliente. Cabe mencionar que el usuario monitoreo también cuenta con esta funcionalidad implementada.

Figura 6-52: Desactivación alarma generada

12. El usuario monitoreo puede obtener información del usuario cliente al presionar la opción “CLIENTES” como se muestra en la Figura 6-53.

Figura 6-53: Opción “CLIENTES” interface web usuario monitoreo

13. Al ejecutar esta acción, el usuario monitoreo selecciona el usuario cliente del que desea obtener la información necesaria para su localización. Presionando el botón “OBTENER INFORMACION” se desplegará una ventana que contiene la información del cliente en cuestión como se muestra en la Figura 6-54.

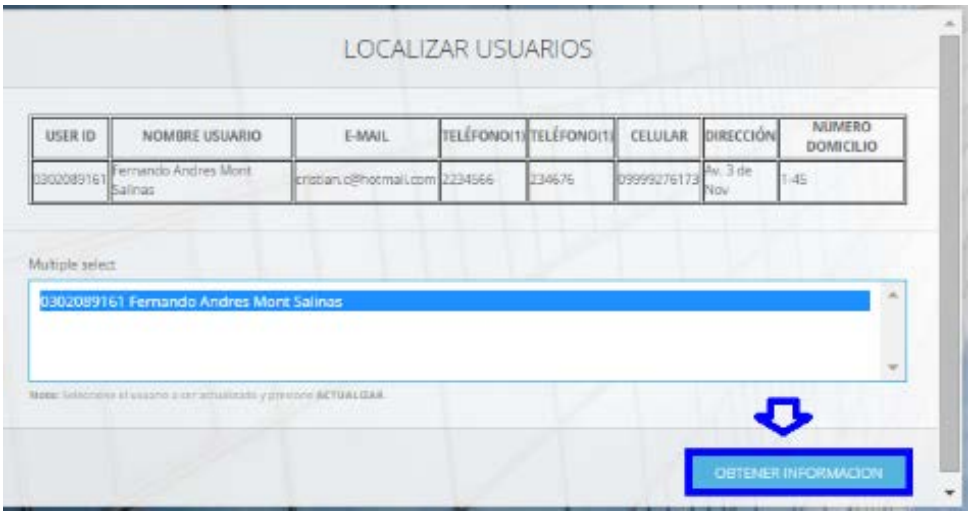


Figura 6-54: Opción “OBTENER INFORMACION” interface web monitoreo

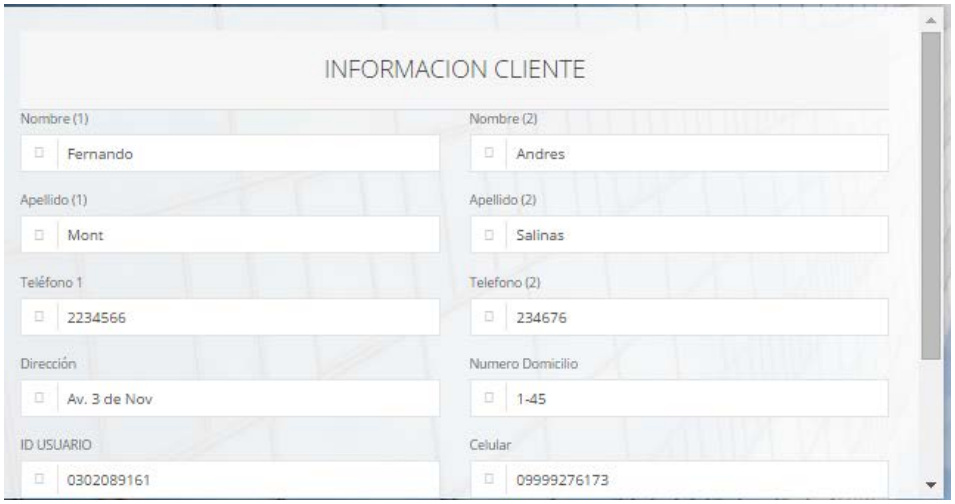


Figura 6-55: Información cliente

14. Al presionar la opción “DESACTIVAR SISTEMA” (Figura 6-56), en la interface web cliente, el sistema se normaliza como se observa en las Figura 6-57. El color de la tabla ha cambiado a verde, lo que indica que el sistema se encuentra no alarmado. Esta acción se refleja tanto en la interface web cliente como en la interface web monitoreo (Ver Figura 6-57, Figura 6-58).

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

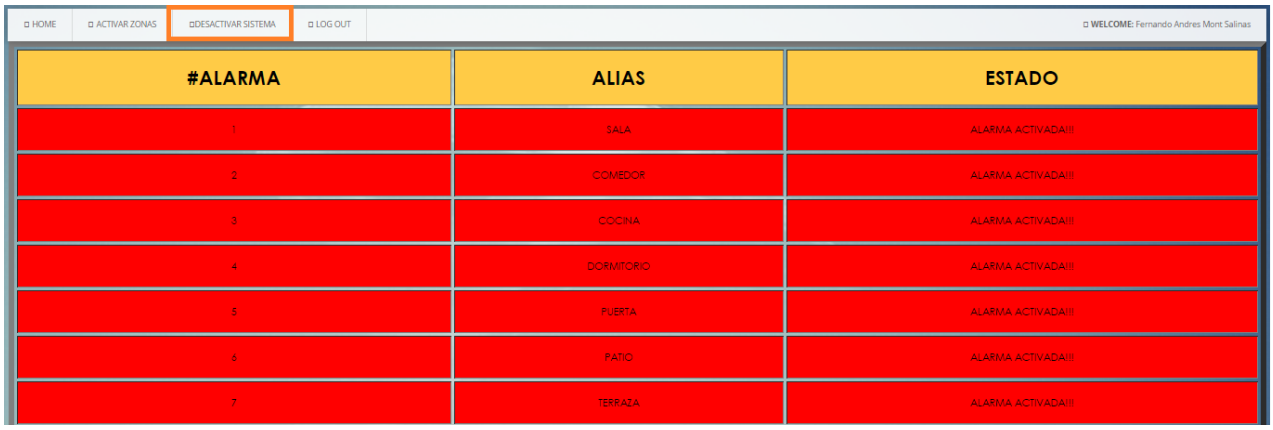


Figura 6-56: Desactivar sistema

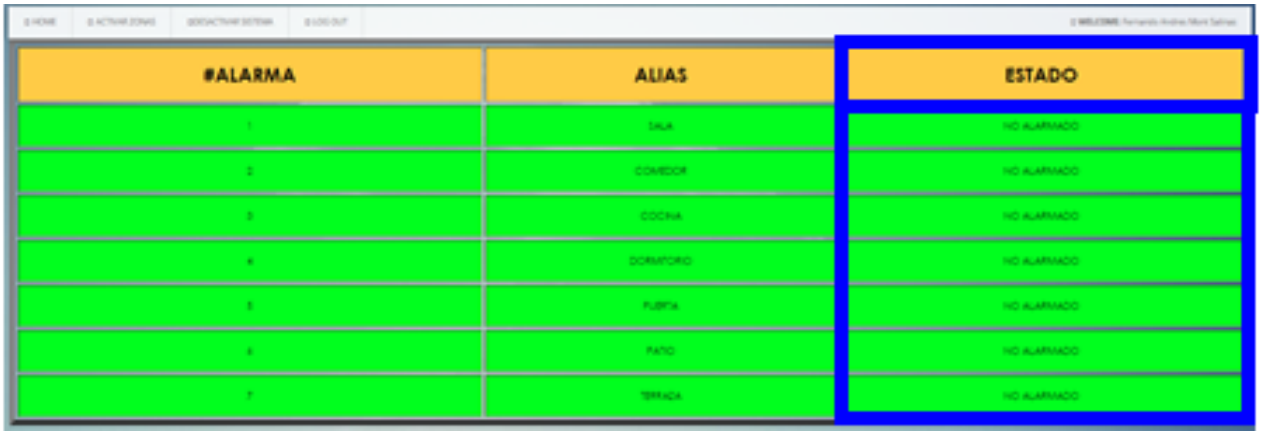


Figura 6-57: Estado de alarmas normalizado interface web cliente

Figura 6-58: Estado de alarmas normalizado interface web monitoreo

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Prueba botón de pánico

1. Como prueba final se procede a la activación de la opción “PANICO” desde la interface web cliente (Figura 6-59). El usuario cliente presiona está opción cuando necesita asistencia inmediata por parte del usuario monitoreo. Esta acción pondrá a todos los sensores en estado “ALARMADO”. Este estado se refleja en la ventana de monitoreo, interface web cliente y monitoreo mostrado en las Figuras 6-60 y 6-61.

Figura 6-59: Estado de alarmas normalizado interface web monitoreo

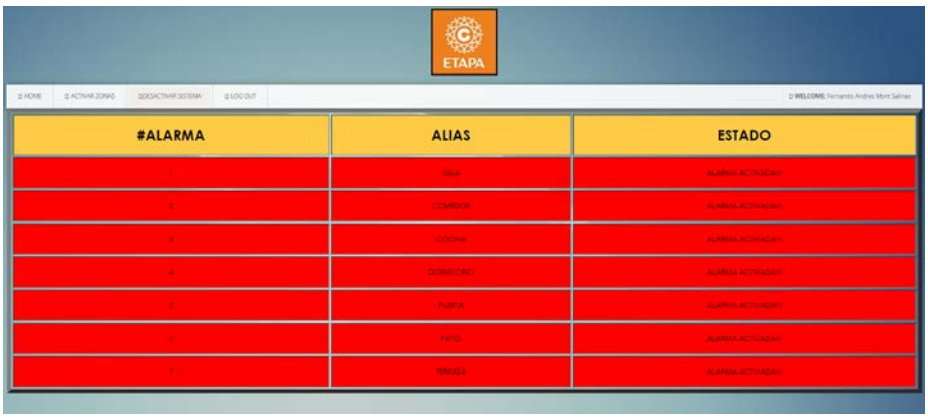


Figura 6-60: Alarmas generada por el botón “PANICO” interface web cliente

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Figura 6-61: Alarmas generada por el botón “PÁNICO” interface web monitoreo

2. Para normalizar nuevamente el sistema se sigue el proceso de desactivación descrito anteriormente en el punto 12 del punto anterior.
3. Al ingresar a la pestaña “Video” (Figura 6-47), se presenta una lista de los clientes que están registrados en el sistema. Se escoge a un usuario que tenga configurado su cámara y al hacer clic en “OBTENER INFORMACION” (Figura 6-62), se visualiza el video en vivo del usuario (Figura 6-63).

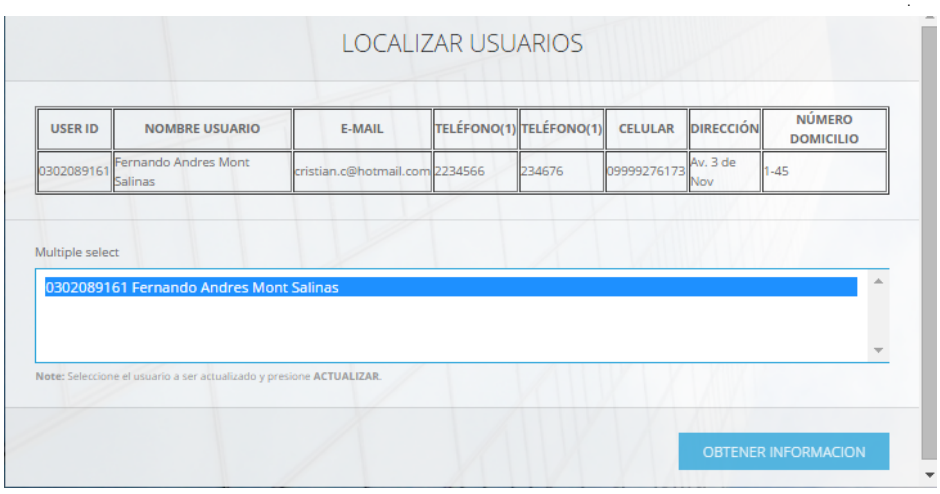


Figura 6-62: Lista de usuarios al pulsar la pestaña “Video” de la interface web monitoreo

Figura 6-63: Visualización de la cámara IP desde la interface web monitoreo.

4. Para probar la visualización en vivo desde la interface web usuario cliente, se debe hacer clic en la pestaña “Video” (Figura 6-46). Esta acción abre una ventana donde se visualiza la cámara IP en vivo (Figura 6-64).

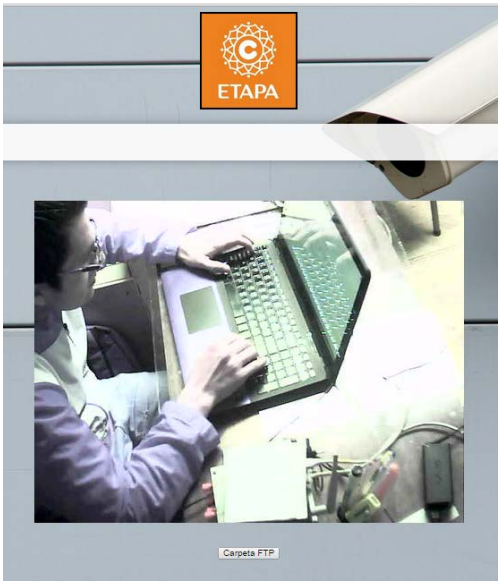


Figura 6-64: Visualización de la cámara IP desde la interface web cliente.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

5. Para probar el almacenamiento de imágenes en el servidor a través del protocolo FTP, se hace clic en el botón “Carpeta FTP” (Figura 6-64). Esta acción inicia la sesión en el servidor FTP para ese usuario (Figura 6-65), donde se encuentran la carpeta con las imágenes capturadas en detección de movimiento, en caso que un evento sea registrado por la cámara.

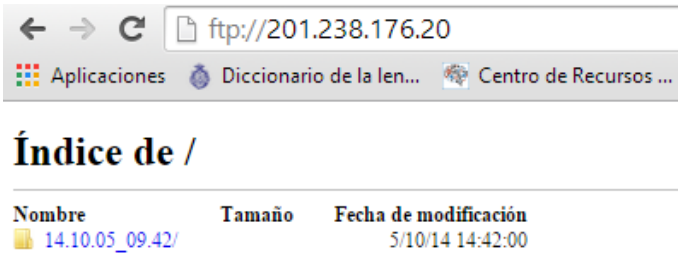


Figura 6-65: Sesión en el servidor FTP

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 7

ANALISIS DE COSTOS

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 7 ANÁLISIS DE COSTOS

7.1 Costos de la aplicación cliente

Una vez implementada la solución, se pueden obtener los costos totales del prototipo, para ello se consideran los costos por separado de la “aplicación cliente” y la “aplicación servidor”, cabe recalcar que en el precio final se ha incluido el IVA (12%).

7.1.1 Costos de la Central de Alarma

Los costos de elaboración de la Central de Alarma se establecen en la Tabla 7-1. Se consideran los módulos: GSM, sensores, gestión de energía, interface y Ethernet. En el caso de los módulos diseñados se considera solo los costos de los elementos utilizados.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CANTIDAD	DESCRIPCION	P. UNIT	P. TOTAL
1	Pic 18F45K22	$ 6.97	$ 6.97
1	Regulador de 3,3V 0,8A LM1117T-3	$ 1.69	$ 1.69
1	Conector RJ45 POS H PCB	$ 0.58	$ 0.58
1	Peineta 1 fila 16 pos.	$ 0.11	$ 0.11
1	Peineta 1 fila 16 pos. angular	$ 0.43	$ 0.43
1	Peineta hembra	$ 0.71	$ 0.71
2	Transistor IRF620 Mosfet 200V 6A	$ 0.97	$ 1.94
1	Baquelita 10x20	$ 1.54	$ 1.54
1	IDC 2X5	$ 0.58	$ 0.58
3	Borneras 3 Pines PCB	$ 0.32	$ 0.96
2	Peineta 2 filas 20 Pos.	$ 0.23	$ 0.47
2	Peineta 1 fila 40 Pos.	$ 0.31	$ 0.62
1	Sócalo de 8 pines	$ 0.07	$ 0.07
1	Sócalo de 40 pines	$ 0.26	$ 0.27
1	Bornera 2 Pines PCB	$ 0.21	$ 0.21
1	Bornera 3 Pines PCB	$ 0.32	$ 0.32
1	Resistencia 120 Ohm 1/4W	$ 0.02	$ 0.02
1	Resistencia 10 Kohm 1/4W	$ 0.02	$ 0.02
1	Pulsante Normal, 2 Pines	$ 0.39	$ 0.39
1	Cristal 4 MHz	$ 0.70	$ 0.70
2	Capacitor Cerámico 22 pF 50V	$ 0.08	$ 0.16
4	Capacitor Cerámico 0,1uF 50V	$ 0.08	$ 0.36
1	Condensador 3300 uF 50V	$ 1.34	$ 1.34
1	Trimer 5 Kohm	$ 0.67	$ 0.67
6	Diodos	$ 0.09	$ 0.53
1	Bornera 3P	$ 0.31	$ 0.31
1	Bornera 2P	$ 0.22	$ 0.22
1	LM317	$ 0.71	$ 0.71
2	Resistencias 10 Kohm	$ 0.03	$ 0.05
6	Condensadores Cerámicos 10uF	$ 0.06	$ 0.38
1	Módulo GSM Cuatribanda	$ 66.00	$ 66.00
7	Disipador TO-220 1 Agujero	$ 0.50	$ 3.50
2	Opto Acoplador PC817	$ 0.35	$ 0.70
1	Diodo Rectificador	$ 0.11	$ 0.11
1	Módulo Ethernet ENC28J60	$ 11.00	$ 11.00
		TOTAL	**$ 89.35**

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Tabla 7-1: Costos de los elementos de la Central de Alama

7.1.2 Costos del Panel de Usuario

En la Tabla 7-2 se muestra en detalle el costo del panel de usuario.

ELEMENTOS DEL PANEL DEL USUARIO			
CANTIDAD	**DESCRIPCION**	**P. UNIT**	**P. TOTAL**
1	Peineta hembra de 40 pines	$ 1.08	$ 1.08
1	Peineta macho de 40 pines	$ 0.92	$ 0.92
5	Resistencias de 10 K	$ 0.02	$ 0.10
2	Resistencias de 120	$ 0.02	$ 0.04
1	Resistencia de 220	$ 0.02	$ 0.02
1	Capacitor 10 nF 50V	$ 0.05	$ 0.05
1	Regulador de 5V 1A 7805T	$ 0.55	$ 0.55
1	Integrado Max 488	$ 3.17	$ 3.17
1	Potenciometro de 20K	$ 0.10	$ 0.10
1	Pulsante normal, 2 pines	$ 0.39	$ 0.39
1	Sócalo de 20 pines	$ 0.14	$ 0.14
1	PIC 18F14K22	$ 3.96	$ 3.96
1	Sócalo de 8 pines	$ 0.07	$ 0.07
1	Conector RJ45 POS H PCB	$ 0.58	$ 0.58
1	Baquelita de 8x13 - 1 capa	$ 2.20	$ 2.20
1	LCD 16X2	$ 10.56	$ 10.56
1	Teclado matricial de 4x4	$ 8.92	$ 8.93
1	Peineta 1 fila 12 POS, ANGULAR	$ 0.33	$ 0.33
4	IDC 2X10	$ 0.58	$ 2.32
10	Borneras	$ 0.13	$ 1.34
		TOTAL	**$ 36.85**

Tabla 7-2: Costos del Panel de Usuario

7.1.3 Costos de los periféricos de la Central de Alarma

Para estos costos se consideran todos los periféricos que interactúan con la Central de Alarma, cada uno de ellos se los puede comprar independientemente de la Central de Alarma.

PERIFERICOS DE LA CENTRAL DE ALARMA			
CANTIDAD	DESCRIPCION	P. UNIT.	P. TOTAL
1	Bateria de 12V	$ 13,20	$ 13,20
1	Transformador a 12V	$ 7,04	$ 7,04
1	Sensor de movimiento	$ 10,56	$ 10,56
1	Sensor magnético	$ 1,76	$ 1,76
1	Sirena	$ 5,80	$ 5,80
1	Camara IP Wireless/Wired	$ 58,93	$ 58,93
		TOTAL	$ 97,29

Tabla 7-3: Costos de los periféricos de la Central de Alarma

7.1.4 Costos de los Materiales

En estos costos se consideran los materiales utilizados para la elaboración de la tarjeta de la Central de Alarma, del panel del usuario y de los módulos. Además el costo de la elaboración de la maqueta, donde se prueba el funcionamiento del sistema.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

HERRAMIENTAS - MATERIALES			
CANTIDAD	DESCRIPCION	P. UNIT	P. TOTAL
1	Broca HSS Alemana 5/32"	$ 0,66	$ 0,66
1	Broca HSS Alemana 1/32"	$ 0,66	$ 0,66
1	Pintura en Spray Ohio	$ 1,76	$ 1,76
1	Broca Alemana 1/64	$ 0,75	$ 0,75
1	Broca HSS Alemana 1/32"	$ 0,66	$ 0,66
1	Broca HSS Alemana 3/64"	$ 0,66	$ 0,66
1	Broca 3"	$ 1,19	$ 1,19
1	Broca 2"	$ 1,06	$ 1,06
4	Tornillos estrellas	$ 0,09	$ 0,35
16	A/P	$ 0,03	$ 0,03
16	Tuercas	$ 0,03	$ 0,03
1	Tornillo	$ 0,03	$ 0,03
4	Tuercas	$ 0,02	$ 0,08
3	Percloruro férrico	$ 0,54	$ 1,61
3	Cable UTP 2 pares	$ 0,35	$ 1,06
1	Conector doble	$ 0,58	$ 0,58
1	Cable plano de 40 hilos	$ 2,26	$ 2,26
2	Pegamento	$ 1,43	$ 2,86
1	Impresión de adhesivo	$ 10,71	$ 10,71
5	Piezas madera	$ 12,05	$ 12,05
1	Spray	$ 2,46	$ 2,46
1	Brocha #1	$ 0,90	$ 0,90
2	Bisagras	$ 1,57	$ 1,57
3	Cable gemelo 2x20 Incable	$ 0,21	$ 0,63
3	Cable telefónico 2x22 interior	$ 0,14	$ 0,41
		TOTAL	$ 45,01

Tabla 7-4: Costos de los elementos y materiales utilizados

7.2 Costos de la aplicación servidor

En los costos de “aplicación servidor” se debe recalcar que para el proyecto se utilizó únicamente software de distribución libre y gratuita, por lo cual no hubo gastos en cuanto a la “aplicación servidor”.

7.3 Costo Total de la solución

El costo total del sistema de seguridad, incluido IVA, fue de $250,30 y sus costos están distribuidos en: costos de la “aplicación servidor”, costos de la “aplicación cliente”, costos de periféricos. Para el costo

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

final del proyecto no se considera los costos de los materiales y herramientas utilizadas ($ 45,01), como se observa en la Tabla 7-5.

HARDWARE	P. TOTAL
Costos de la Central de Alarma	$ 89,35
Costos del Panel de Usuario	$ 36,85
Costos de Periféricos	$ 97,29
SOFTWARE	**P. TOTAL**
Costos de Software	$ -
SUBTOTAL	$ 223,48
IVA 12%	$ 26,82
COSTO TOTAL	**$ 250,30**

Tabla 7-5: Costo Total del prototipo

7.4 Resultados

Puesto que se realizaron consultas en cuanto al costo de un kit básico de seguridad electrónica que incluyera: panel, teclado, batería, transformador, sirena, gabinete, sensor de movimiento y sensor magnético a varias empresas que ofrecen el servicio de seguridad electrónica en la ciudad de Cuenca. Se obtuvo una tabla comparativa del precio ofrecido por estas empresas y el costo del prototipo (Tabla 7-9). En el Anexo F, se encuentran los costos de cada uno de los kits ofrecidos por las empresas consultadas.

En las Tablas 7-6, 7-7 y 7-8 se observan los costos de kits similares al kit básico que se utilizó en el prototipo.

EMPRESA	SERVICIO		PRECIO
JASETRON SEGURIDAD.	Gabinete metálico + Central de Alarma		$ 109,43
	Tarjeta de 4-8 zonas		
	Teclado DSC + cargador de baterias		
	Transformador de 16,5 VA - 40VA		$ 12,29
	Batería de respaldo 12V 4AH		$ 23,21
	Sirena 30W dos tonos		$ 17,00
	1 contactos magnéticos para puertas		$ 3,90
	1 Sensores de movimiento antimascota		$ 18,13
		TOTAL	**$ 183,96**

Tabla 7-6: Costo de un kit básico 1

EMPRESA	SERVICIO		PRECIO
SEVIMAN Cía Ltda.	Gabinete metálico + Central de Alarma		$ 180,00
	Tarjeta de 4-8 zonas		
	Teclado LED		
	Transformador de 16,5 VA - 40VA		
	Batería de respaldo 12V 4AH		
	Sirena 30W dos tonos		
	1 contactos magnéticos para puertas ($25,00)		$ 25,00
	1 Sensores de movimiento antimascota ($10)		$ 10,00
		TOTAL	$ 215,00

Tabla 7-7: Costo de un kit básico 2

EMPRESA	SERVICIO		PRECIO
G4S	Gabinete metálico + Placa disuasiva		$ 149,00
	Tarjeta de 8 zonas + Central de Alarma		
	Teclado LED		
	Transformador de 16,5 VA - 40VA		
	Batería de respaldo 12V 4AH		
	Sirena 30W dos tonos		
	Sensor magnético simple		
	Sensor de movimiento		
	1 Sensor infrarojo Analógico Paradox PRO 110'		$ 19,00
	1 Magnetico Adhesivo Blanco/Café		$ 3,00
	1 Botón de Pánico		$ 5,00
		TOTAL	$ 176,00

Tabla 7-8: Costo de un kit básico 3

En base a los resultados obtenidos se concluye que los costos de un sistema de seguridad electrónica que incluya los elementos de un kit básico esta entre los $170 y $220, el precio varía de acuerdo a la marca de los equipos y el tipo de sensores utilizados.

El costo total del prototipo es de $250,30, pero hay que tener en cuenta que se incluye el costo de la cámara IP, con lo cual se reduciría su valor aproximadamente a los $200.

EMPRESA	P. TOTAL
JASETRON SEGURIDAD	$ 183.96
SEVIMAN Cía. Ltda.	$ 215.00
G4S	$ 176.00
PROTOTIPO	$ 250.30

Tabla 7-9: Comparación entre sistemas de seguridad

El costo del prototipo sin cámara IP se encuentra en un valor intermedio de los costos de los sistemas de seguridad electrónica consultados, con lo cual no hay diferencia con estos.

Hay que tener en cuenta que el prototipo a diferencia de los sistemas de seguridad electrónica consultados cuenta con una cámara IP y una aplicación web para el acceso del usuario.

CAPÍTULO 8

CONCLUSIONES Y RECOMENDACIONES

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

CAPÍTULO 8 CONCLUSIONES Y RECOMENDACIONES

8.1 Conclusiones

El diseño de la “aplicación cliente”, basada en la idea de reutilizar al máximo los elementos de un kit de seguridad convencional, encamino a la solución a estandarizarse y ser compatible con varias soluciones, haciendo del prototipo una solución fácil de instalar, accesible para los clientes y amigable con el usuario.

Debido al uso de protocolos de diferentes características y a la secuencialidad del microcontrolador, los retardos en la comunicación entre la central de alarma y la “aplicación servidor” oscilan entre 5 y 10 segundos, considerados como muy elevados.

El desarrollo de PCBs con el método seleccionado y el uso de integrados THT, permite elaborar tarjetas electrónicas a bajo precio y de manera fácil, pero hay que considerar también otros métodos actuales e integrados SMD que ayudarías a reducir su tamaño y tener mejores acabados, sin embargo se trata de un prototipo así que la elección fue la adecuada.

Debido a las funcionalidades desarrolladas en la aplicación de software para la adquisición de información del estado de los sensores, se ha podido desarrollar un sistema confiable que permita al cliente tener un conocimiento del estado de su hogar.

La implementación de un método de autentificación para el ingreso a la aplicación, permite que solamente los usuarios registrados puedan acceder al sistema. Evitando que usuarios no autorizadas puedan alterar el funcionamiento del sistema.

Los costos de licenciamiento por la utilización de software libre y código a nivel de Hardware y Software han sido reducidos. Lo que permite obtener un sistema de seguridad accesible para un cliente común.

8.2 Recomendaciones

La gestión de energía del sistema, es una de los puntos más importantes y de mayor complejidad, a la hora de diseñar los requerimientos de energía se recomienda sobre dimensionar el consumo, para no tener inconvenientes en caso de realizar cambios al sistema.

El microcontrolador seleccionado pese a sus altas prestaciones, a medida que se avanza en la programación y se implementan funcionalidades, no cumplió con su propósito debido a que se utilizó por completo la memoria de programa. De modo que no da la oportunidad de continuar con su desarrollo y brindar escalabilidad. Se recomienda seleccionar microcontroladores de gamas más altas.

Ya que la “aplicación servidor” debe tener una disponibilidad 24 x 7, éste debe estar localizado en un lugar que cuente con el correcto suministro y respaldo de energía, constante ventilación para evitar el sobrecalentamiento de los equipos, seguridad y disponer de la conectividad necesaria para brindar el servicio.

En caso de que se requiera manejar un mayor número de clientes, se tiene que considerar aumentar el procesamiento y la capacidad de almacenamiento del servidor.

BIBLIOGRAFÍA

[1] http://www.monografias.com/trabajos-pdf5/sistema-alarmas/sistema-alarmas.shtml [Online]

[2] http://www.monografias.com/trabajos5/datint/datint.shtml [Online]

[3] http://www.ecured.cu/index.php/Modelo_de_Referencia_OSI [Online]

[4] http://es.wikipedia.org/wiki/Cliente-servidor [Online]

[5] http://www.mikroe.com/mikroc/pic/ [Online]

[6] http://www.microchip.com/DevelopmentTools [Online]

[7] http://en.wikipedia.org/wiki/Commercial_software [Online] 17,11.2014

[8] http://en.wikipedia.org/wiki/Free_software [Online] 23,11,2014

[9] **Jon Duckett**, **Beginning,** Web Programming with HTML, XHTML, and CSS: 2008 Wiley Publishing, Inc, Apress

[10] **Kenneth L. Calvert, Michael J. Donahoo,** TCP/IP Sockets in Java, Second Edition: Practical Guide for Programmers: February 22, 2008, Second Edition

[11] **Harvey M. Deitel, Paul J. Deitel,** Java How to Program: Prentice Hall January 6, 2007, Seventh Edition

[12] **Antonio Goncalves**, Beginning Java EE 6 with GlassFish 3**:** 2010, 2nd Edition 2010

[13] **Robert J. Brunner,** JSP Practical Guide for Java Programmers: Morgan Kaufmann, 1 edition (September 24, 2003)

[14] **Jayson Falkner, Kevin Jones,** Servlets and JavaServer Pages: 2004 Pearson Education, Second Edition

[15] htttp://www.genbetadev.com/bases-de-datos/fundamento-de-las-bases-de- datos-modelo-entidad-relacion [Online]

[16] http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure [Online]

[17] http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=security SSLKeytool. [Online]

[18] www.certificadodigital.com.ar/download/GUsuario.pdf [Online]

[19] http://es.wikipedia.org/wiki/File_Transfer_Protocol#Servidor_FTP [Online]

[20] DATABASE SYSTEMS, Desing, Implementation and Management, Coronel, Morris, Rob, 2011 Cengage Learning

[21] http://es.wikipedia.org/wiki/C%C3%A1mara_IP0 [Online]

[22] http://www.3ts.it/ipcam.asp [Online]

[23] http://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html [Online] 10,09,2012

[24] http://omnitron.com.ec/nuestrosProductos.php?id=6 [Online]

[25] http://es.wikipedia.org/wiki/Serial_Peripheral_Interface [Online]

[26] http://victorhckinthefreeworld.wordpress.com/2013/03/25/las-7-mejores-distribuciones-de-gnulinux-del-2013/ [Online] 25,03,2013

[27] http://alsofidesworld.blogspot.com/2012/08/seguridad-de-una-red-de-area-local.html [Online]

[28] **DUANE K. FIELDS, MARK A**. Web Development with JavaServer Pages, 2002 Manning Publications Co.

[29] **Tim Downey, Springer-Verlag**, Guide to Web development with Java – Understanding Website Creation Tim Downey; Springer-Verlag London Limited 2012.

[30] http://www.genbetadev.com/bases-de-datos/fundamento-de-las-bases-de-datos-modelo-entidad-relacion [Online]

[31] JSP Practical Guide for Java Programmers, Robert J. Brunner, 2003.

[32] http://www.edu4java.com/es/web/web30.html [Online]

[33] http://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html [Online]

[34] http://img.clasf.co.ve/2014/04/14/Transformador-Para-Alarmas-Paradox-Dsc-Honeywell-20140414040852.jpg [Online]

[35] http://ultracell.net/datasheets/UL4-12.pdf [Online]

[36] http://mla-s2-p.mlstatic.com/sensor-magnetico-alarma-puerta-ventana-porton-abertura-detec-12673-MLA20064543416_032014-O.jpg [Online]

[37] http://www.geeetech.com/wiki/images/f/fa/GPRS2.jpg [Online]

[38] http://www.botnroll.com/img/p/818-2298-thickbox.jpg [Online]

[39] http://akizukidenshi.com/img/goods/C/I-05380.JPG [Online]

[40] http://yourduino.com/sunshop2/images/products/large_317_max485.jpg [Online]

[41] http://security.stackexchange.com/questions/36993/can-i-spoof-ipaddresses-when-attempting-to-brute-force-a-login [Online]

[42] http://mlm-s1-p.mlstatic.com/pantalla-lcd-16x2-azul-display-arduino-10321-MLM20028068477_012014-O.jpg [Online]

[43] http://www.tiendaelectronica.com.ve/1122-1378-thickbox/teclado-matricial-4x4.jpg [Online]

[44] IP Wireless Wired Camera, User Manual

[45] http://tecnotinker.blogspot.com/2012/07/uso-del-modulo-ethernet-enc28j60-con.html [Online]

[46] https://www.digitalocean.com/community/tutorials/how-to-configure-vsftpd-to-use-ssl-tls-on-an-ubuntu-vps [Online]

[47] http://www.alcancelibre.org/staticpages/index.php/procedimiento-instalar-centos6 [Online]

[48] http://wiki.centos.org/About/Product#fndefa8ee1384a09cba71d01121bda643ecc2993b9e62-16 [Online]

[49] http://www.arduinopassion.com/wp-content/uploads/2012/07/arduino-ethernet-module.jpg [Online]

[50] http://www.foscamchile.cl/information.php?info_id=1 [Online]

[51] http://cms.dsc.com/download.php?t=3&file=http://cms.dsc.com/media/products/master/LC-100-PI.tif [Online]

[52] http://microrevolucion.blogspot.com/2012/10/importancia.html [Online]

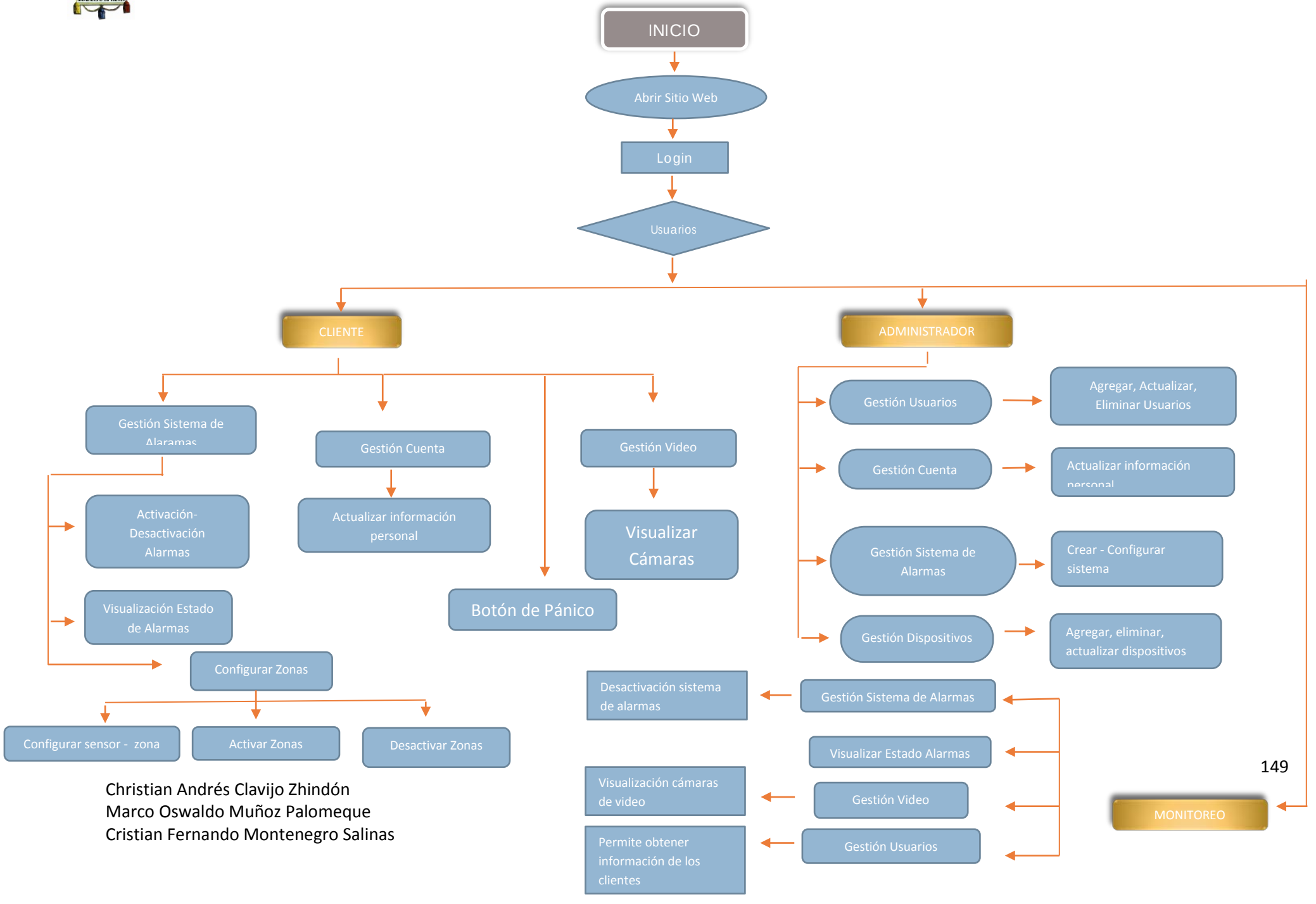
[53] http://www.davidghedini.com/pg/entry/install_glassfish_3_1_on. [Online]

ANEXOS

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

ANEXO A: FUNCIONALIDADES USUARIOS DEL SISTEMA

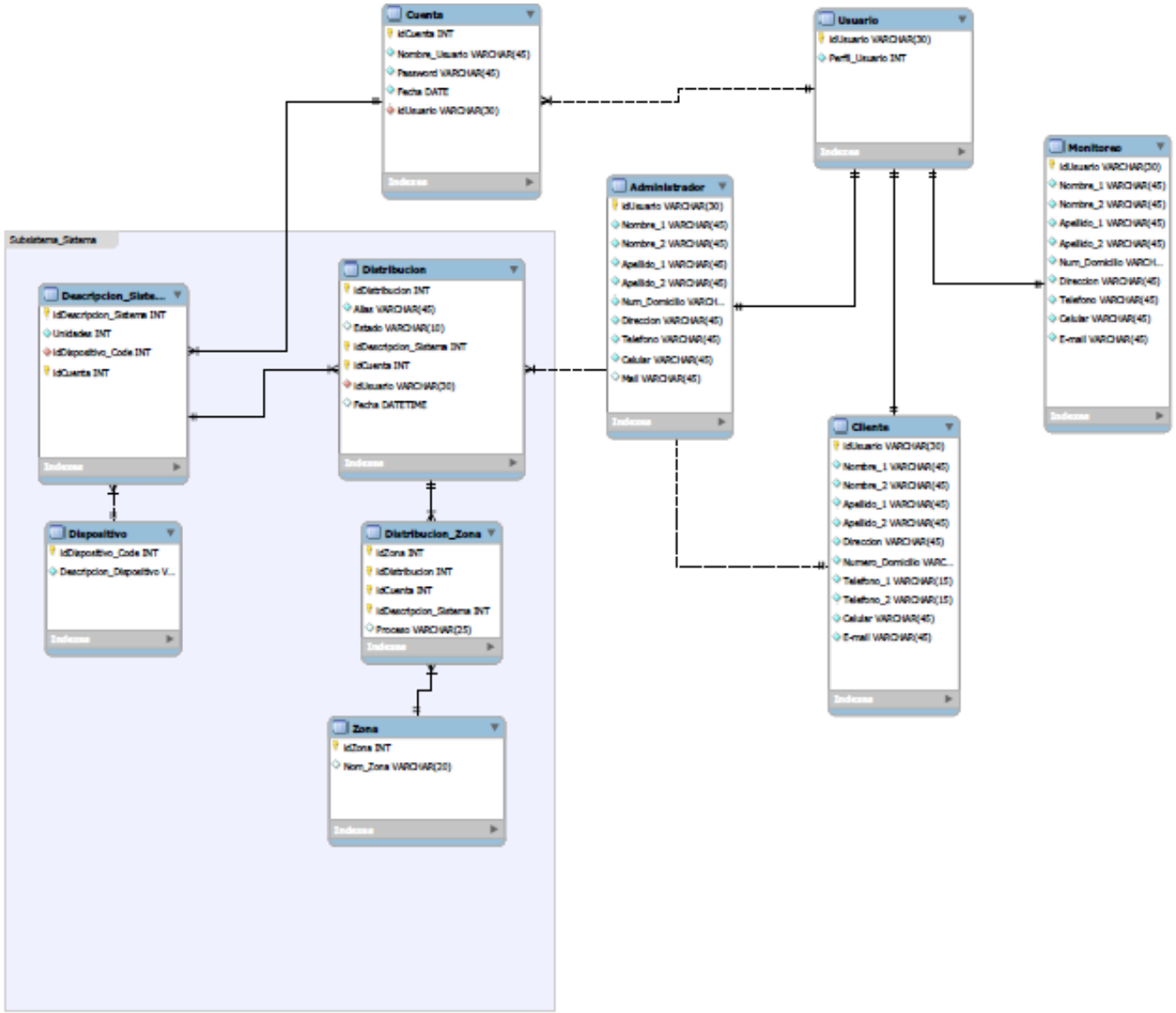
Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas



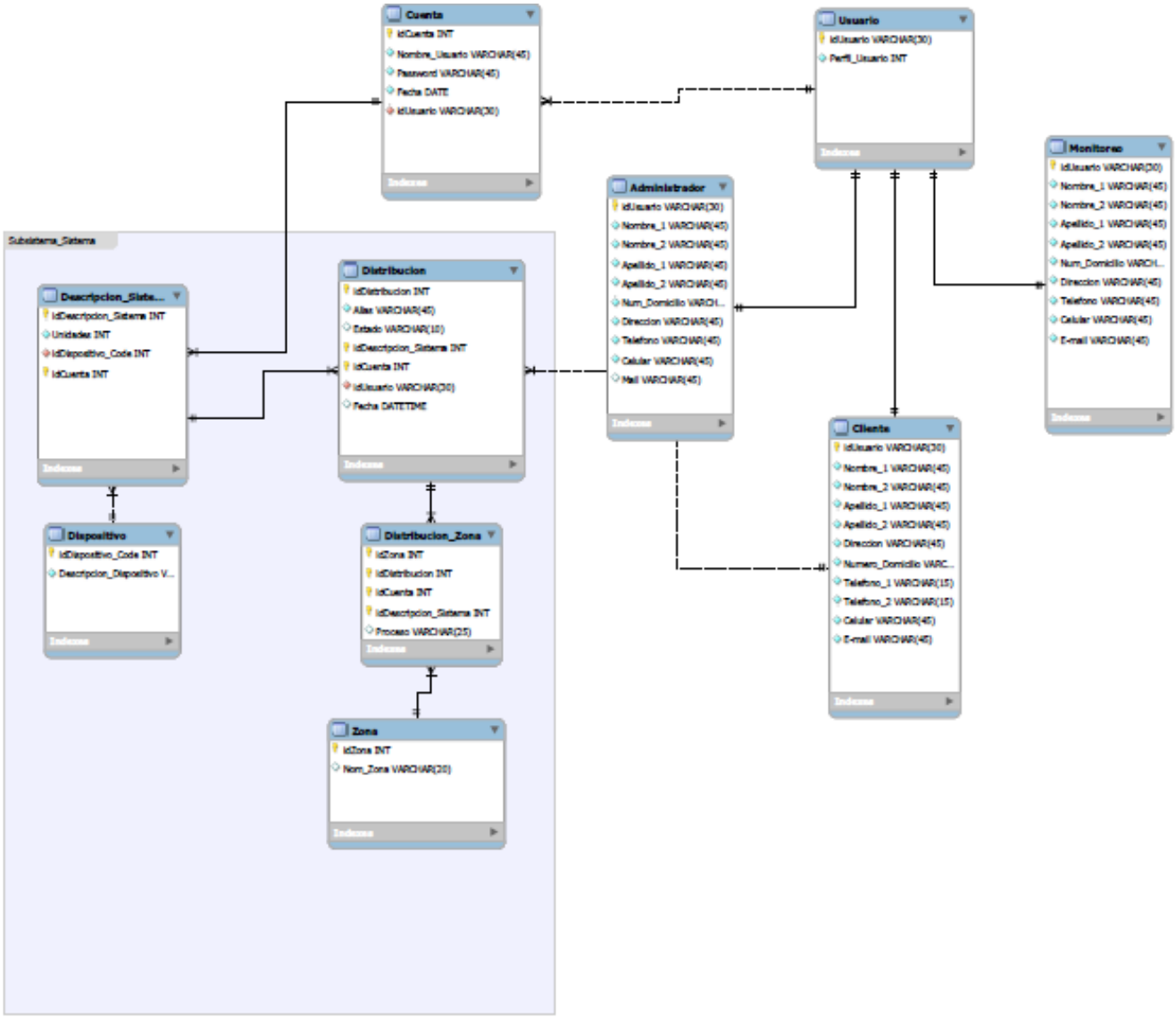
Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

ANEXO B: MODELO ENTIDAD RELACIÓN SISTEMA DE SEGURIDAD DOMICILIARIA

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas



Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas


Cuenta
idCuenta INT
Nombre_Usuario VARCHAR(45)
Password VARCHAR(45)
Fecha DATE
idUsuario VARCHAR(30)
Usuario
idUsuario VARCHAR(30)
Perfil_Usuario INT
Monitoreo
idUsuario VARCHAR(30)
Nombre_1 VARCHAR(45)
Nombre_2 VARCHAR(45)
Apellido_1 VARCHAR(45)
Apellido_2 VARCHAR(45)
Num_Domicilio VARCH...
Direccion VARCHAR(45)
Telefono VARCHAR(45)
Celular VARCHAR(45)
E-mail VARCHAR(45)
Administrador
idUsuario VARCHAR(30)
Nombre_1 VARCHAR(45)
Nombre_2 VARCHAR(45)
Apellido_1 VARCHAR(45)
Apellido_2 VARCHAR(45)
Num_Domicilio VARCH...
Direccion VARCHAR(45)
Telefono VARCHAR(45)
Celular VARCHAR(45)
Mail VARCHAR(45)
Subsistema_Sistema
Descripcion_Siste...
idDescripcion_Sistema INT
Unidades INT
idDispositivo_Code INT
idCuenta INT
Distribucion
idDistribucion INT
Alias VARCHAR(40)
Estado VARCHAR(10)
idDescripcion_Sistema INT
idCuenta INT
idUsuario VARCHAR(30)
Fecha DATETIME
Dispositivo
idDispositivo_Code INT
Descripcion_Dispositivo V...
Distribucion_Zona
idZona INT
idDistribucion INT
idCuenta INT
idDescripcion_Sistema INT
Proceso VARCHAR(25)
Zona
idZona INT
Nom_Zona VARCHAR(20)
Cliente
idUsuario VARCHAR(30)
Nombre_1 VARCHAR(45)
Nombre_2 VARCHAR(45)
Apellido_1 VARCHAR(45)
Apellido_2 VARCHAR(45)
Direccion VARCHAR(45)
Numero_Domicilio VARC...
Telefono_1 VARCHAR(15)
Telefono_2 VARCHAR(15)
Celular VARCHAR(45)
E-mail VARCHAR(45)

ANEXO C: CONFIGURACIÓN CÁMARA IP

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Configuración de la cámara IP

Para configurar la cámara IP de marca FOSCAM primero se instala el software *IP Camera Tool* desde el CD que provee el fabricante, este permite identificar la dirección IP privada que le asigna el modem a la cámara IP.

Una vez que es asignada una dirección IP a la cámara se ingresa a la interface web de la cámara para realizar las configuraciones (Figura C-1). Se puede acceder a la cámara desde el software *IP Camera Tool* o digitando la dirección IP en la barra de direcciones de un navegador (Internet Explorer, Google Chrome, Safira o Firefox). Por defecto el usuario y contraseña es*: Admin* y sin contraseña.

Figura C-1: Interface Web Server de la cámara.

Ahora se configura una IP estática a la cámara que no esté en el rango de direcciones asignadas por DHCP del modem, asegurándose que este en el rango admitido por el modem. Se le asigna la dirección IP 192.168.1.15 y el

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

puerto 8081, para que no interfiera con el servidor de aplicaciones que usa los puertos 80 y 8080 (Figura C-2).

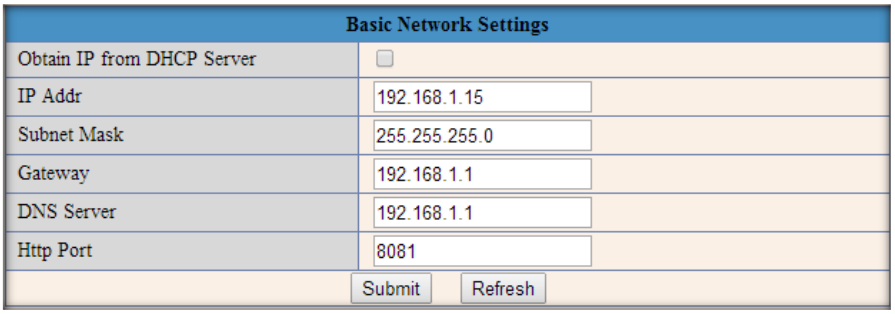


Figura C-2: Asignación de una IP estática a la cámara.

Para que la cámara pueda conectarse inalámbricamente a la red, se debe hacer una búsqueda de la red Wireless del modem mediante el botón Scan. Una vez identificada la red, se selecciona el tipo de encriptación y la contraseña de la red (Figura C-3).

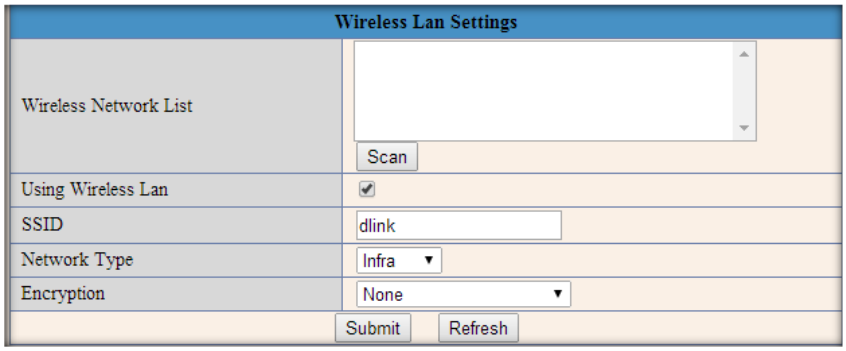


Figura C-3: Configuración de Wireless LAN.

Para acceder a la cámara desde Internet se necesita tener configurado el servicio DDNS (DNS dinámico), el cual permite actualizar en tiempo real la información de nombres de dominio (Figura C-4). Este asigna un nombre de dominio de internet a la dirección IP dinámica, de esta forma es posible conectarse a la cámara fuera de la red privada, a través de internet.

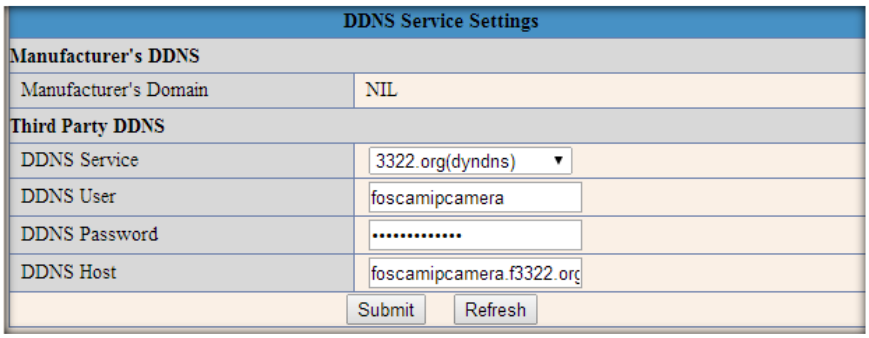


Figura C-4: Configuración del Servicio DDNS

Utilizando el servicio ofrecido gratuitamente por la empresa china PubYun, se puede obtener el servicio DDNS, para esto se crea una cuenta en la página web www.pubyun.com (Anexo E).

Para tener almacenamiento de imágenes, cuando se tiene activada la opción Detección de Movimiento, en el servidor; se configura el servicio FTP de la cámara. Donde se coloca la dirección del servidor FTP, se ingresa el puerto, el nombre de usuario, contraseña y la dirección exacta de la carpeta a donde se subirán las imágenes (Figura C-5).

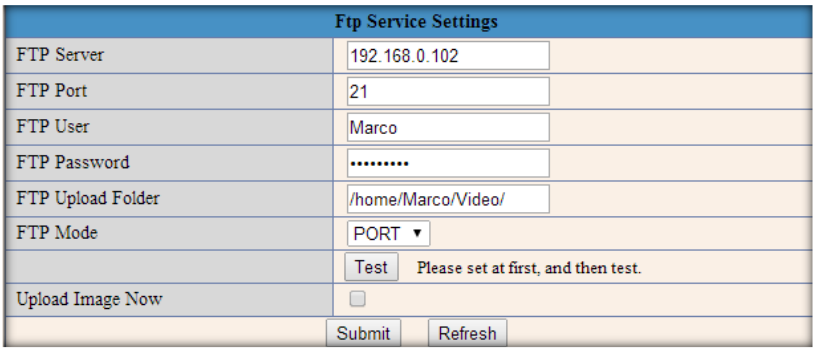


Figura C-5: Configuración del servidor FTP

ANEXO D: CONFIGURACIÓN EN EL MODEM

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Configuración en el Modem

En el modem se debe realizar algunas configuraciones, en este caso se configura un modem de marca D-Link. Para habilitar el *port fordwarding,* que hace que la dirección IP de la cámara y el puerto asignado estén habilitados, se ingresa a la página de configuración del modem ingresando la IP del Gateway. En las opciones de configuración (Figura D-1), en la opción *Device Info*, se obtiene toda la información de configuración del modem que el ISP utiliza (Figura D-2).

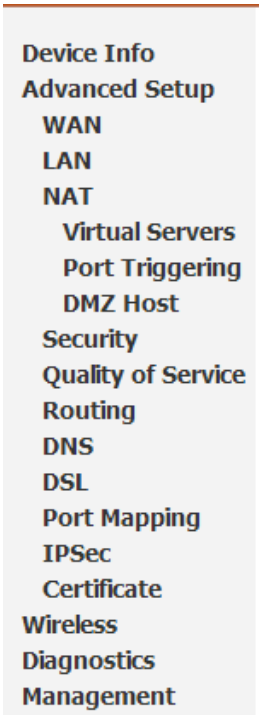
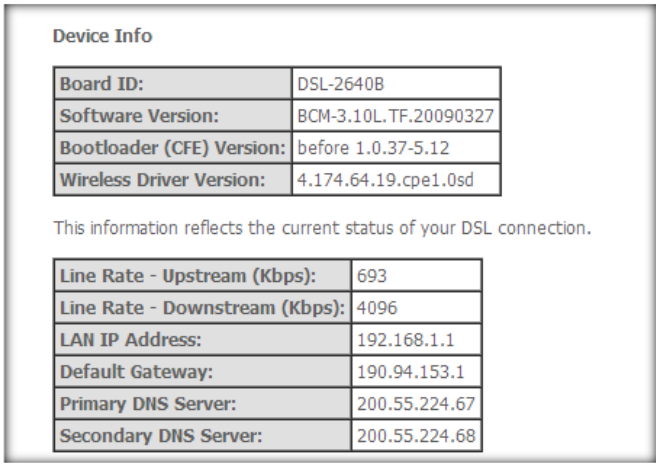


Figura D-1: Opciones de Configuración del Modem D-Link

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas



Device Info

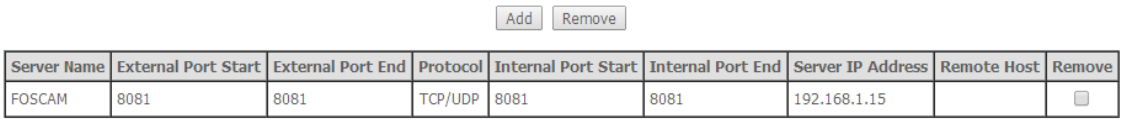
Board ID:	DSL-2640B
Software Version:	BCM-3.10L.TF.20090327
Bootloader (CFE) Version:	before 1.0.37-5.12
Wireless Driver Version:	4.174.64.19.cpe1.0sd

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	693
Line Rate - Downstream (Kbps):	4096
LAN IP Address:	192.168.1.1
Default Gateway:	190.94.153.1
Primary DNS Server:	200.55.224.67
Secondary DNS Server:	200.55.224.68

Figura D-2: Información del Modem D-Link

Se agrega la dirección IP estática y el puerto asignado a la cámara (Figura D-3), en la opción Virtual Servers. En este caso se configura con el nombre *FOSCAM*, el puerto el 8081 y la IP 192.168.1.15.

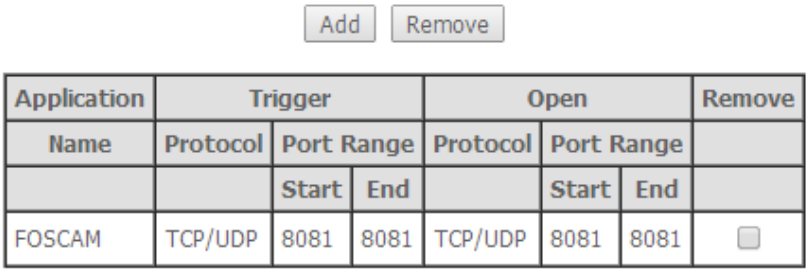


Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
FOSCAM	8081	8081	TCP/UDP	8081	8081	192.168.1.15		

Figura D-3: Configuración de la dirección IP de la cámara

Para habilitar el puerto en el modem, se debe configurar el protocolo y la aplicación que lo utiliza. En la opción *Port Triggering*, se ingresa el nombre de aplicación que se le asigno (FOSCAM), el puerto de inicio y fin (en caso de un rango de puertos, si no se escribe el mismo puerto) 8081 y el protocolo a usar TCP/UDP (Figura D-4).



Add Remove

Application	Trigger			Open			Remove
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	
FOSCAM	TCP/UDP	8081	8081	TCP/UDP	8081	8081	

Figura D-4: Configuración del puerto 8081

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

ANEXO E: CONFIGURACIÓN DEL SERVICIO DDNS

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Configuración de la cuenta en PubYun

Se debe acceder a la página web www.pubyun.com para crear una cuenta. Se debe hacer clic según indica la flecha en la Figura E-1.

Figura E-1: Página de Inicio de PubYun

En la ventana que aparece se ingresa los datos del usuario que va a crear la cuenta, como nombre de usuario, correo, password, etc… (Figura E-2). Finalmente aparece un mensaje indicando que se ha creado la cuenta exitosamente (Figura E-3).

Figura E-2: Datos del Usuario para la cuenta

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

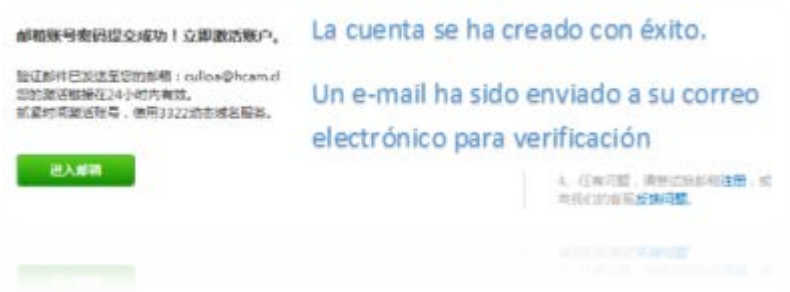


Figura E-3: Confirmación de la cuenta

En el correo ingresado llega un mensaje para confirmar la cuenta. Se hace clic en el enlace enviado que aparece. La página web a la cual envía, es la de PubYun y finalmente se ingresa con el usuario y contraseña.

Figura E-4: Correo de confirmación de la cuenta

Se Ingresa en la cuenta creada en los pasos anteriores, para ello se hace clic donde indica la flecha en la página de inicio (Figura E-5).

Figura E-5: Ingreso a la cuenta creada.

Se ingresa el nombre de usuario y contraseña, respectivamente (Figura E-6). Para crear la dirección para el DDNS, se debe escribir el nombre con el

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

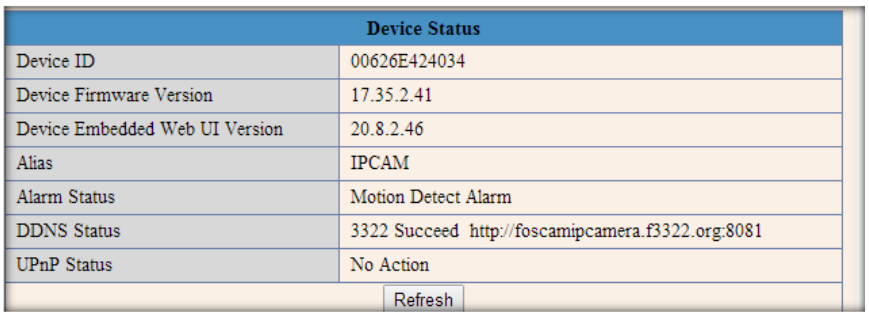
cual se identificará la cámara IP, en este caso se usa ***foscamipcamera***, la empresa PubYun agrega la terminación *.f3322.org. Además se debe asignar el puerto configurado para la cámara IP. Realizado esto se debe confirmar los datos, en la ventana que se abre aparecen la IP Pública del modem, el nombre de la cuenta y la fecha de acceso (Figura E-7).

Figura E-6: Ventana de ingreso de usuario y contraseña

Figura E-7: Verificación que la cuenta se ha creado

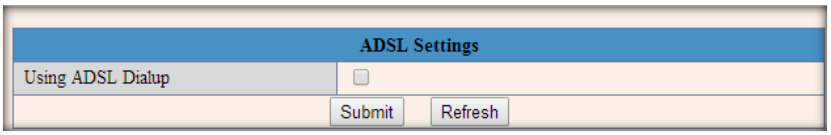
Finalmente se prueba que el servicio de DDNS está funcionando, para esto se debe estar fuera de la LAN, es decir en la WAN (desde internet). Se ingresa en un navegador con la dirección que se asignó al crear la cuenta, en este caso: foscamipcamera.f3322.org:8081.

Al ingresar en el web server de la cámara IP, en *Device Status*, aparece la dirección DDNS (Figura E-8). Adicionalmente se debe confirmar que la casilla de *ADSL Settings* este desmarcada (Figura E-9).



Device Status	
Device ID	00626E424034
Device Firmware Version	17.35.2.41
Device Embedded Web UI Version	20.8.2.46
Alias	IPCAM
Alarm Status	Motion Detect Alarm
DDNS Status	3322 Succeed http://foscamipcamera.f3322.org:8081
UPnP Status	No Action
Refresh	

Figura E-8: Verificación de la configuración de DDNS



ADSL Settings	
Using ADSL Dialup	☐
Submit	Refresh

Figura E-9: Verificación de ADSL Settings

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

ANEXO F: COSTOS DE SISTEMAS DE SEGURIDAD

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Los costos que se observan en las Tablas F1 a F10, son los obtenidos al consultar empresas de seguridad electrónica de Cuenca en los meses de septiembre y octubre del 2013. Para algunos casos no se detallan los costos de cada elemento del kit y se coloca el costo más barato para un sistema de seguridad electrónica, aunque este formado por algunos elementos que no se consideran para el prototipo.

EMPRESA	SERVICIO		PRECIO
MEI	Alarmas		$ 280,00
	Video Vigilancia		
	Control de Acceso		
	Cercos Eléctricos		
	Motores para Garage		
	Porteros Eléctricos		
		TOTAL	$ 280,00

Tabla F-1: Precio de un kit de seguridad 1

EMPRESA	SERVICIO		PRECIO
PROTEC	Alarmas		$ 500,00
	Circuito Cerrado de TV		
	Control de Acceso		
	Cercos Eléctricos		
	Motores para Garage		
	Porteros Eléctricos		
	Automatización de puertas		
	Respuesta Armada		$ 18,50
		TOTAL	$ 518,50

Tabla F-2: Precio de un kit de seguridad 2

EMPRESA	SERVICIO		PRECIO
SEGTRONICS	Alarma Antirrobo		$ 290,00
	Circuito Cerrado de TV 3 cámaras		
	Control de Acceso		
	Cercos Eléctricos		
	Motores abre puertas C.R.		
	Porteros Eléctricos - Video		
	Cámara + DVR		$ 110,00
		TOTAL	$ 400,00

Tabla F-3: Precio de un kit de seguridad 3

EMPRESA	SERVICIO		PRECIO
ALARM STOP	Alarmas		$ 350,00
	Monitoreo		$ 12,32
	Control de Acceso		$ -
	Cercos Eléctricos		$ -
	Circuito cerrado de TV		$ -
	Porteros Eléctricos		$ -
	Automatización de puertas		$ -
	Respuesta Armada		$ 17,92
		TOTAL	$ 362,32

Tabla F-4: Precio de un kit de seguridad 4

EMPRESA	SERVICIO		PRECIO
ATS	Alarmas		$ 650,00
	Monitoreo		
	Control de Acceso		
	Cercos Eléctricos		
	Circuito cerrado de TV		
	Porteros Eléctricos		
	Automatización de puertas		
	Respuesta Armada		
		TOTAL	$ 650,00

Tabla F-5: Precio de un kit de seguridad 5

EMPRESA	SERVICIO		PRECIO
DISMELCOM, Safetown Cía Ltda.	Gabinete metálico con pintura electrostática		$ 268,00
	Tarjeta de 8 zonas		
	Teclado LED para visualización de zonas		
	Transformador de 16,5 VA		
	Batería de respaldo 12V 4AH		
	Sirena 30W		
	Automatización de puertas		
	2 Enforcer Magnético café		
	2 Sensores de movimiento interior antimascota 220 KG		
	Instalación y programación		
	Cables y materiales de montaje		
	IVA		$ 32,16
		TOTAL	$ 300,16

Tabla F-6: Precio de un kit de seguridad 6

EMPRESA	SERVICIO		PRECIO
SEGURIPRIV Cía Ltda.	Cámaras de Seguridad		$ -
	Alarmas para domicilios		$ 320,00
	Detectores de incendios		$ -
	Monitoreo de alarmas		$ -
		TOTAL	$ 320,00

Tabla F-7: Precio de un kit de seguridad 7

EMPRESA	SERVICIO		PRECIO
JASETRON SEGURIDAD.	Gabinete metálico + Central de Alarma		$ 109,43
	Tarjeta de 4-8 zonas		
	Teclado DSC + cargador de baterias		
	Transformador de 16,5 VA - 40VA		$ 12,29
	Batería de respaldo 12V 4AH		$ 23,21
	Sirena 30W dos tonos		$ 17,00
	4 contactos magnéticos para puertas		$ 15,60
	2 Sensores de movimiento antimascota		$ 36,26
	Instalación + punto de montaje + cableado		$ 77,00
	Programación del sistema		$ 10,00
	Monitoreo via telefonica, Supervición General		
	IVA		$ 36,09
		TOTAL	$ 336,88

Tabla F-8: Precio de un kit de seguridad 8

EMPRESA	SERVICIO		PRECIO
SEVIMAN Cía Ltda.	Gabinete metálico + Central de Alarma		$ 180,00
	Tarjeta de 4-8 zonas		
	Teclado LED		
	Transformador de 16,5 VA - 40VA		
	Batería de respaldo 12V 4AH		
	Sirena 30W dos tonos		
	3 contactos magnéticos para puertas ($25,00)		$ 30,00
	5 Sensores de movimiento antimascota ($10)		$ 125,00
	Instalación + programación del sistema		$ 40,00
	Cables (Multipar, gemelos, etc)		$ 50,00
	IVA		$ -
		TOTAL	$ 425,00

Tabla F-9: Precio de un kit de seguridad 9

EMPRESA	SERVICIO		PRECIO
G4S	Gabinete metálico + Placa disuasiva		$ 149,00
	Tarjeta de 8 zonas + Central de Alarma		
	Teclado LED		
	Transformador de 16,5 VA - 40VA		
	Batería de respaldo 12V 4AH		
	Sirena 30W dos tonos		
	Sensor magnético simple		
	Sensor de movimiento		
	1 Sensor infrarojo Analógico Paradox PRO 110'		$ 19,00
	1 Magnetico Adhesivo Blanco/Café		$ 3,00
	1 Botón de Pánico		$ 5,00
	Instalación + programación del sistema		$ 64,00
	Cables (Multipar, gemelos, etc)		$ -
	IVA		$ -
		TOTAL	$ 213,00

Tabla F-10: Precio de un kit de seguridad 10

ANEXO G: SELECCION DE EQUIPOS

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

Transformador: Es un elemento necesario en los circuitos electrónicos debido a que reduce la tensión de 110V a 16V. Además debido a su estructura aislante protege al usuario en su manipulación. En la Figura G-1 se muestra el transformador.

Figura G-1: Transformador DSC 16.5VAC. (Tomado de [34])

Batería: Elemento que no puede faltar en sistemas de seguridad, puesto que ayuda a respaldar el suministro de energía en caso de corte de energía eléctrica o si el sistema requiere corriente adicional. Trabaja a 12V y puede proporcionar hasta 4A por una hora. Una imagen de la batería se muestra en la Figura G-2.

Figura G-2: Batería VRLA 12V 4AH. (Tomado de [35])

Sensor de Movimiento: Dispositivo principal para la detección de intrusos en los sistemas de seguridad. Es un sensor PIR (Passive Infra Red) que detecta la presencia de personas mediante la temperatura del ambiente. Su respuesta ante la detección es ON-OFF funcionando como un relé. En la Figura G-3 se muestra la imagen del sensor.

Figura G-3: Sensor de movimiento DSC PIR. (*Tomado de [51])*

Sensor Magnético: Dispositivo ampliamente usado en los sistemas actuales, su principal función es detectar la apertura de puertas y ventanas. En la Figura G-4 se muestra la imagen del sensor.

Figura G-4: Sensor magnético. (Tomado de [36])

Sirena: Es un elemento de efecto sonoro ideal para notificar la ocurrencia de eventos, como en este caso detección de intrusos. En la Figura G-5 se ilustra la imagen de la sirena.

Figura G-5: Sirena 12V 0.75mA

Módulo GSM - SIM900: Es una solución completa GSM/GPRS que cumple con el estándar y comandos AT, además ofrece conectores DIP para interacción con el microcontrolador. Para su elección se consideraron las bandas de

trabajo y la disponibilidad de información sobre su funcionamiento. En la Figura G-6 se muestra una foto del SIM900 con su antena.

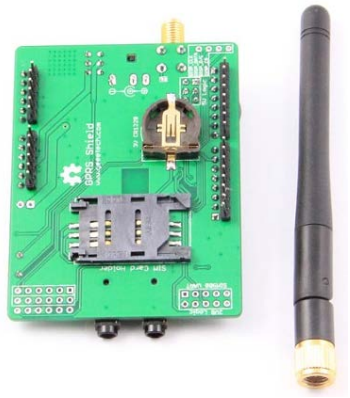


Figura G-6: Modulo GSM SIM900. (Tomado de [37])

ENC28J60: Elemento antes descrito en el módulo Ethernet, su elección de debe al costo frente a otras soluciones, además que existen muchos ejemplos y librerías para su implementación.

PIC18F45K22: Es un Microcontrolador de altas prestaciones y encargado de manejar la central de alarma. Aquí se programan todas las funciones antes descritas en el módulo central. Para esto esté PIC cuenta con 40 pines, 30 canales /*-analógicos para conversión analógico digital, 64Kbytes de memoria de programa, oscilador interno, Timer, SPI, Interrupciones, 2 EUSART. En la Figura G-7 se ilustra el PIC18F45K22.

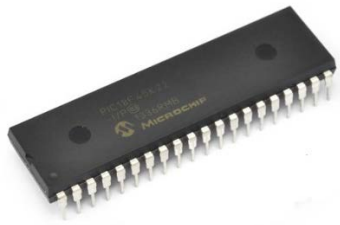


Figura G-7: Imagen del PIC18F45K22. (Tomado de [52])

PIC18F14K22: Como se mencionó antes controla el funcionamiento del terminal, aquí se implementa PP para comunicación con el modulo central. Su elección se debe al número de pines y a la RAM necesaria para el manejo del LCD. Es el cerebro del terminal, controla el manejo del LCD, teclado y

comunicación con el Modulo Central. En la Figura G-8 se muestra la imagen del Microcontrolador PIC.

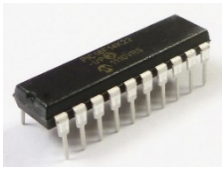


Figura G-8: Imagen del PIC18F14K22. (Tomado de [52])

Cámara IP Wireless: Para el prototipo se escogió una cámara IP que cumpla las siguientes características básicas:

- Transmisión de video en vivo.
- Compresión de video optimizado (MJPEG).
- Web Server embebido.
- Soporte de red inalámbrica (WI-FI/802.11/b/g).
- Soporte de IP dinámica (DDNS).
- Detección de movimiento.
- Soporte de captura de imágenes.
- Soporte de múltiples protocolos: HTTP/TCP/IP/UDP/SMTP/DDNS/SNTP/DHCP/FTP
- Soporte de encriptación: WEP/WPA/WPA2.

En la Figura G-9 se muestra su imagen.

Figura G-9: Cámara IP Wireless marca Foscam. (Tomado de [50])

ANEXO H: DISEÑO ELECTRÓNICO DE LOS MÓDULOS DE LA CENTRAL DE ALARMA

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

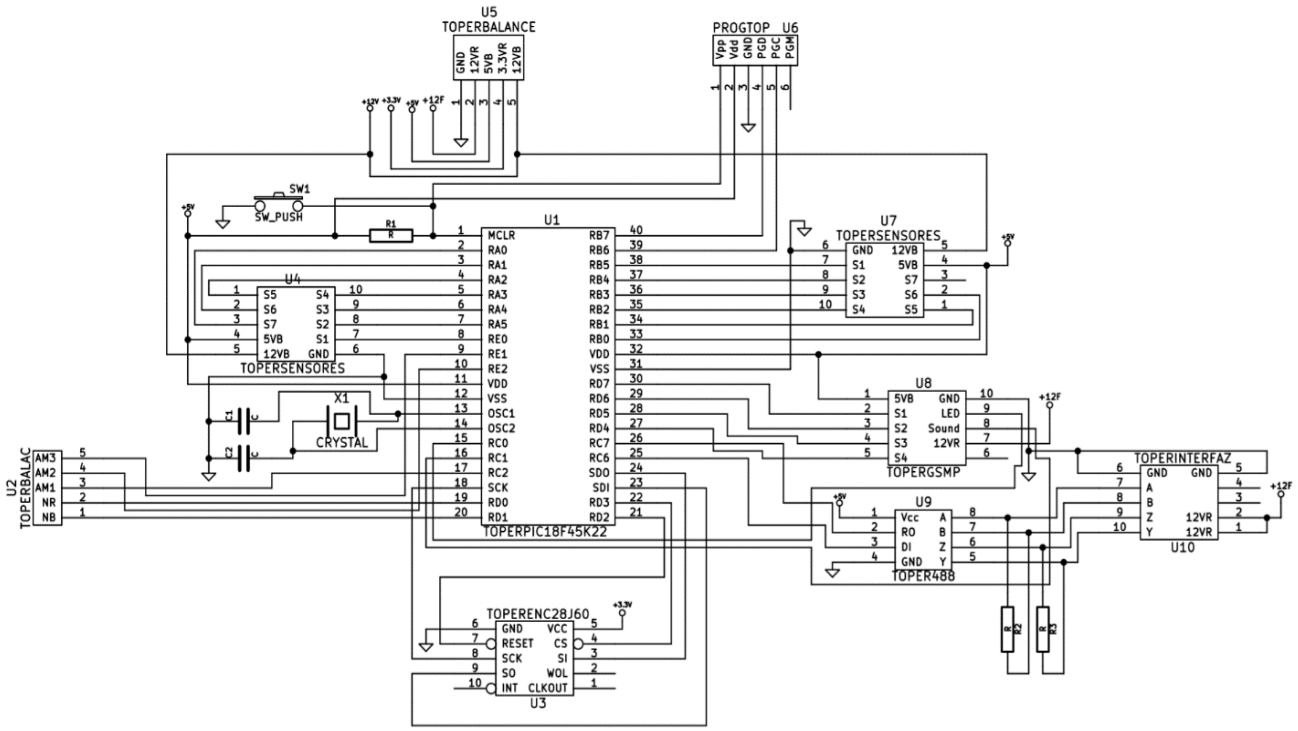


Figura H-1: Diseño electrónico del módulo Central

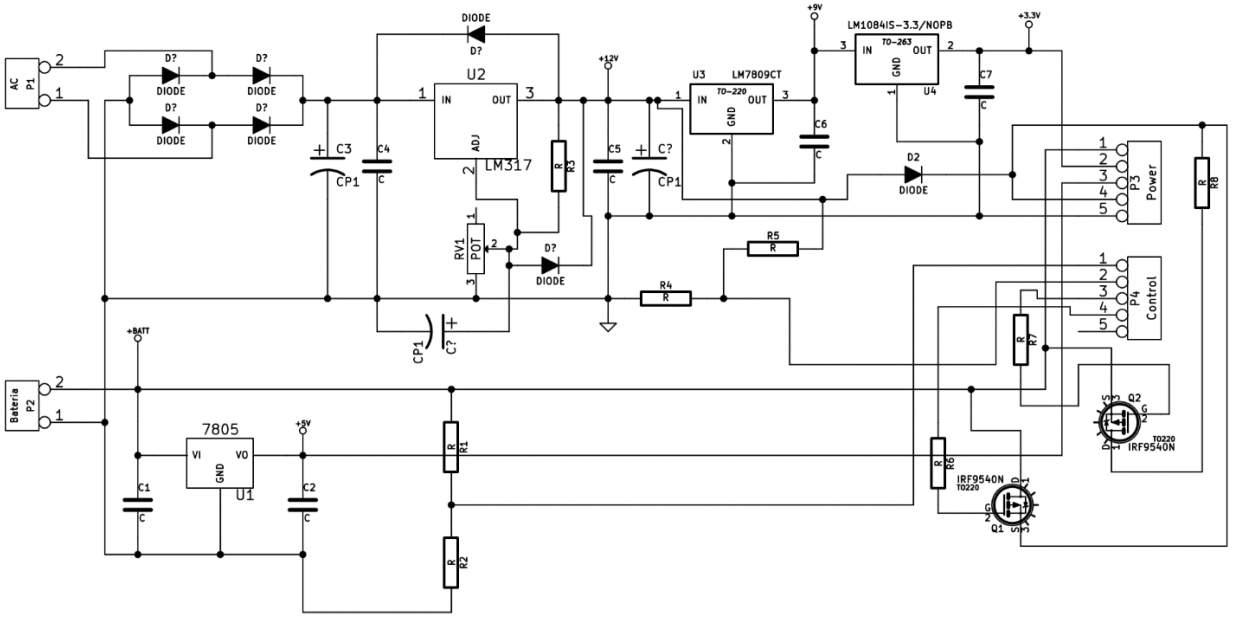


Figura H-2: Diseño electrónico del módulo gestión de energía.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

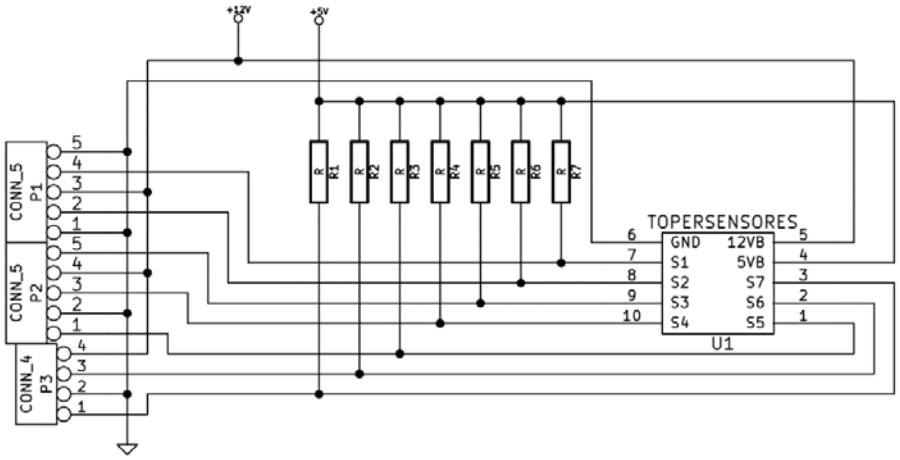


Figura H-3: Diseño electrónico del módulo Sensores

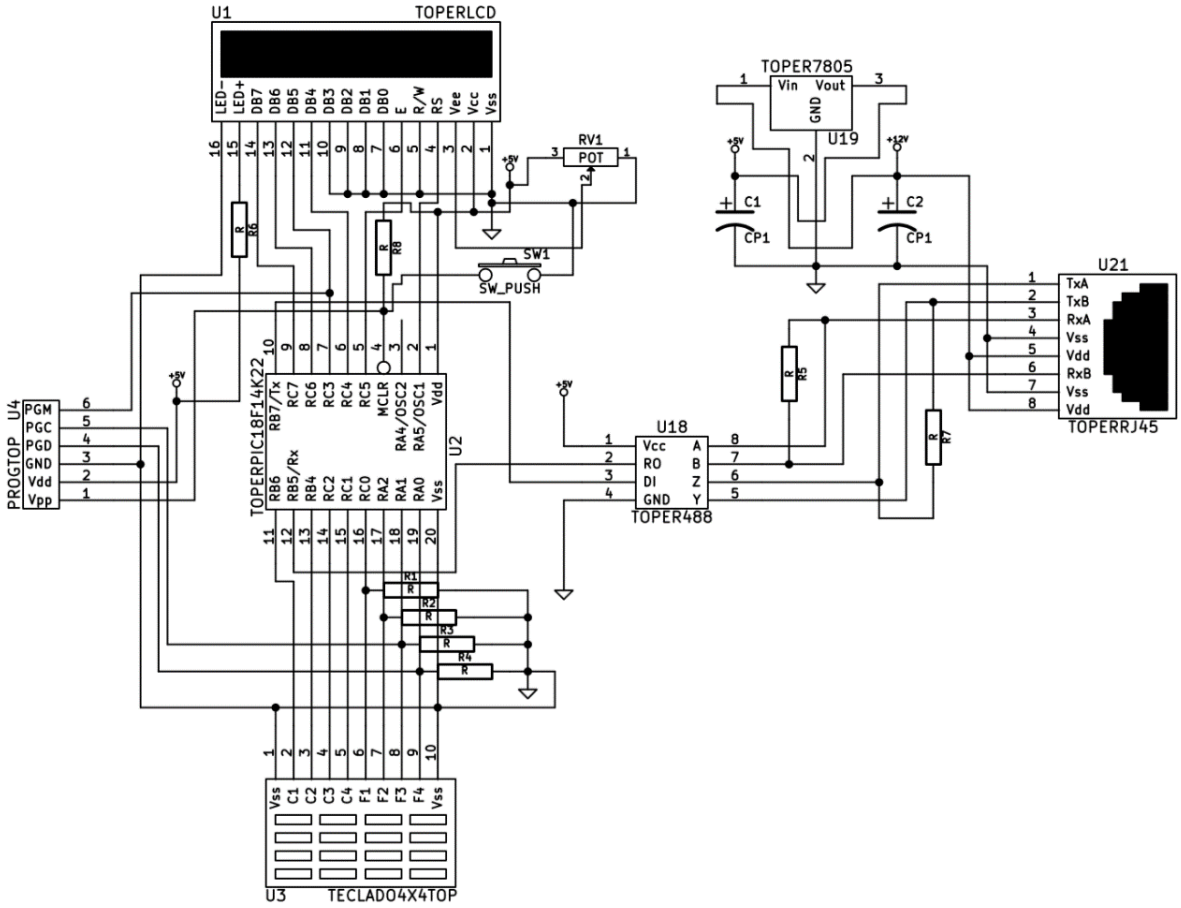


Figura H-4: Diseño electrónico del Panel de Usuario.

Christian Andrés Clavijo Zhindón
Marco Oswaldo Muñoz Palomeque
Cristian Fernando Montenegro Salinas

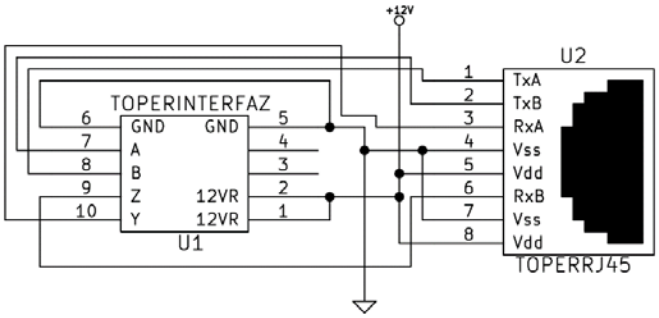


Figura H-5: Diseño del circuito para cambiar el estándar de conector de IDC a RJ45

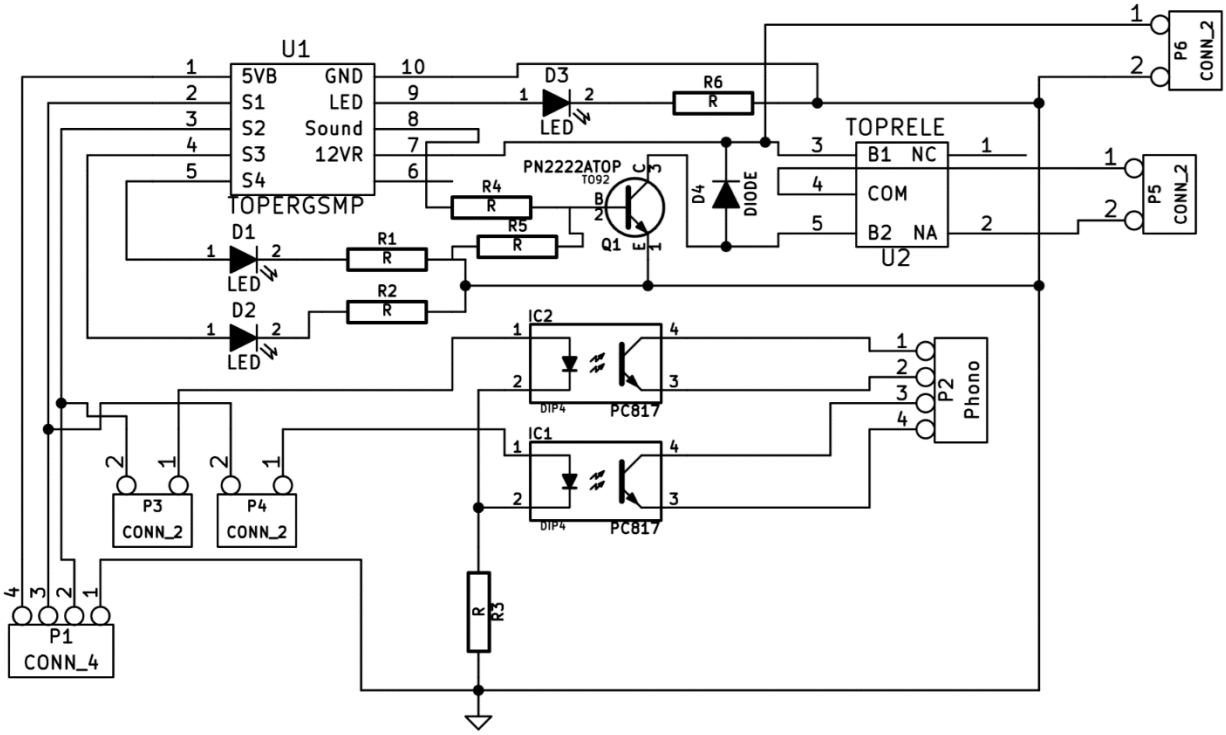


Figura H-6: Diseño electrónico del Módulo GSM-Sonido.